FLORENTIN SMARANDACHE

COLLECTED PAPERS

(Vol. I)

**EDITURA SOCIETĂȚII TEMPUS,
ROMÂNIA, BUCUREȘTI
1996**

FLORENTIN SMARANDACHE

COLLECTED PAPERS

(Vol. I)

EDITURA SOCIETĂŢII TEMPUS
ROMÂNIA, BUCUREŞTI
1996

Director
GEO STROE
40.01.7453379
C.P. 58 – 14
77350 BUCUREȘTI
ROMÂNIA

PRINTED IN ROMANIA
I.S.B.N. 973 – 9205 – 02 – X
Tiraj 1000 ex.
Tipărit la:

COLLECTED PAPERS[1]

(Vol. I)

(articles, notes, generalizations, paradoxes, miscellaneous
in
mathematics, linguistics, and education)

1 Some papers not included in the volume were confiscated by the Secret Police in September 1988, when the author left Romania. He spent 19 months in a Turkish political refugee camp, and emigrated to the United States in March 1990. Despite efforts by his friends, the papers were not recovered...

CONTENTS

A NUMERICAL FUNCTION IN CONGRUENCE THEORY

In this paper we define a function L with will allowus to generalize (separately or simultaneously) some theorems from Numbers Theory obtained by Wilson, Fermat, Euler, Gauss, Lagrange, Leibnitz, Moser, Sierpinski.

§1. Let A be the set $\{m \in \mathbf{Z} \mid m = \pm p^{\beta}, \pm 2p^{\beta}$ with p an odd prime, $\beta \in \mathbf{N}^*$, or $m = \pm 2^{\alpha}$ with $\alpha = 0, 1, 2$, or $m = 0\}$..

Let $m = \varepsilon p_1^{\alpha_1} \dots p_s^{\alpha_s}$ be, with $\varepsilon = \pm 1$, all $\alpha_i \in \mathbf{N}^*$, and $p_1, \dots p_s$ are distinct positive primes.

We construct the FUNCTION $L: \mathbf{Z} \to \mathbf{Z}$,

$$L(x,m) = (x + c_1) \dots (x + c_{\varphi(m)})$$

where $c_1, \dots c_{\varphi(m)}$ are all residues modulo m relatively prime to m, and φ is the Euler's function.

If all distinct primes which divide x and m simultaneously are $p_{i_1}, \dots p_{i_r}$ then:

$L(x,m) \equiv \pm 1 (\operatorname{mod} p_{i_1}^{\alpha_{i_1}} \dots p_{i_r}^{\alpha_{i_r}})$ when $m \in A$ respective by $m \notin A$, and

$$L(x,m) \equiv 0 (\operatorname{mod} m / (p_{i_1}^{\alpha_{i_1}} \dots p_{i_r}^{\alpha_{i_r}}))$$

Noting $d = p_{i_1}^{\alpha_{i_1}} \dots p_{i_r}^{\alpha_{i_r}}$ and $m' = m / d$ we find

$$L(x,m) \equiv \pm 1 + k_1^0 d \equiv k_2^0 m' (\operatorname{mod} \; m)$$

where k_1^0, k_2^0 constituite a particular integer solution of the diophantic equation $k_2 m' - k_1 d = \pm 1$ (the sings are chosen in accordance with the affiliation of m to A). This result

generalizes the Gauss's theorem ($c_1,...c_{\varphi(m)} \equiv \pm 1 (\text{mod } m)$) when $m \in A$ respectively $m \notin A$) (see [1]) which generalized in its turn the Wilson's theorem (if p is prime then $(p-1)! \equiv -1 (\text{mod } m)$).

Proof.

The following two lemmas are trivial:

Lemma 1. If $c_1,...c_{\varphi(p^\alpha)}$ are all residues modulo p^α relatively prime to p^α, with p an integer and $\alpha \in \mathbf{N}^*$, then for $k \in \mathbf{Z}$ and $\beta \in \mathbf{N}^*$ we have also that $.kp^\beta + c_1,...,kp^\beta + c_{\varphi(p^\alpha)}$ constituite all residues modulo p^α relatively prime to it is sufficiently to prove that for $1 \le i \le \varphi(p^\alpha)$) we have $kp^\beta + c_i$ relatively prime to p^α, but this is abviously.

Lemma 2. If $c_1,...c_{\varphi(m)}$ are all residues modulo m relatively prime to m, $p_i^{\alpha_i}$ divides m and $p_i^{\alpha_i+1}$ does not divide m, then $c_1,...c_{\varphi(m)}$ constitute $\varphi(m / p_i^{\alpha_i})$ sistems of all residues modulo $p_i^{\alpha_i}$ relatively prime to $p_i^{\alpha_i}$.

Lemma 3. If $c_1,...c_{\varphi(q)}$ are all residues modulo q relatively prime to q and $(b,q) \sim 1$ then $b + c_1,...,b + c_{\varphi(q)}$ contain a representative of the class $\hat{0}$ modulo q.

Of course, because $(b,q-b) \sim 1$ there will be a $c_{i_0} = q - b$ whence $b + c_i = \mathcal{M}_q$.

From this we have the

Theorem 1. If $\left(x, m / \left(p_{i_1}^{\alpha_{i_1}} ... p_{i_s}^{\alpha_{i_s}}\right)\right)^{\sim 1}$ then

$(x + c_1)...(x + c_{\varphi(m)}) \equiv 0\left(\text{mod}\, m / \left(p_{i_1}^{\alpha_{i_1}} ... p_{i_r}^{\alpha_{i_r}}\right)\right)$

Lemma 4. Because $c_1,\ldots c_{\varphi(m)} \equiv \pm 1 (\bmod m)$ it results that $c_1,\ldots c_{\varphi(m)} \equiv \pm 1(\bmod p_i^{\alpha_i})$, for all i, when $m \in A$ respectively $m \notin A$.

Lemma 5. If p_i divides x and m simultaneously then $(x+c_1)\ldots(x+c_{\varphi(m)}) \equiv \pm 1(\bmod p_i^{\alpha_i})$, when $m \in A$ respectively $m \notin A$. Of course, from the lemmas 2 and 1, respectively 4 we have $(x+c_1)\ldots(x+c_{\varphi(m)}) \equiv c_1,\ldots c_{\varphi(m)} \equiv \pm 1(\bmod p_i^{\alpha_i})$.

From the lemma 5 we obtain the

Theorem 2. If $p_{i_1},\ldots,p_{i_r}$ are all primes which divide x and m simultaneously then $(x+c_1)\ldots(x+c_{\varphi(m)}) \equiv$ $\equiv \pm 1\left(\bmod p_{i_1}^{\alpha_{i_1}}\ldots p_{i_r}^{\alpha_{i_r}}\right)$, when $m \in A$ respectively $m \notin A$.

From the theorems 1 and 2 it results $L(x,m) = \pm 1 + k_1 d = k_2 m'$, where $k_1, k_2 \in \mathbf{Z}$ Because $(d,m') \sim 1$ the diophantia equation $.k_2 m' - k_1 d = \pm 1$ admits integer solutions (the unknowns being k_1 and k_2). Hence $k_1 = m't + k_1^0$ and $k_2 = dt + k_2^0$, with $t \in \mathbf{Z}$, and k_1^0, k_2^0 constitute a particular integer solution of our equation. Thus:

$$L(x,m) = \pm 1 + m'dt + k_1^0 d \equiv \pm 1 + k_1^0 (\bmod m)$$

or

$$L(x,m) = k_2^0 m' (\bmod m)$$

§2. APPLICATIONS

1) Lagrange extended Wilson in the following way: "if p is prime then $x^{p-1} - 1 \equiv (x+1)(x+2)\ldots(x+p-1) \bmod p)$; we shall extend this result to so:

whichever were $m \neq 0, \pm 4$ we have for $x^2 + s^2 \neq 0$ that

$$x^{\varphi(m_s)+s} - x^s \equiv (x+1)(x+2)\ldots(x+|m|-1)(\bmod m)$$

where m_s and s are obtained from the algorithm:

(0) $\begin{cases} x = x_0 d_0 & ;(x_0, m_0) \sim 1 \\ m = m_0 d_0 & ;d_0 \neq 1 \end{cases}$

(1) $\begin{cases} d_0 = d_0^1 d_1 & ;(d_0^1, m_1) \sim 1 \\ m_0 = m_1 d_1 & ;d_1 \neq 1 \end{cases}$

....

(s-1) $\begin{cases} d_{s-2} = d_{s-2}^1 d_{s-1} & ;(d_{s-2}^1, m_{s-1}) \sim 1 \\ m_{s-2} = m_{s-1} d_{s-1} & ;d_{s-1} \neq 1 \end{cases}$

(s) $\begin{cases} d_{s-1} = d_{s-1}^1 d_s & ;(d_{s-1}^1, m_s) \sim 1 \\ m_{s-1} = m_s d_s & ;d_s = 1 \end{cases}$

(see [3] or [4]). For m positive prime we have $m_s = m$, $s = 0$ and $\varphi(m) = m - 1$, that is Lagrange.

2) L. Moser enunciated the following theorem: if p is prime then $(p-1)!a^p + a = \mathcal{M}p$", and Sierpinski (see [2], p.57): "if p is prime then $a^p + (p-1)!a = \mathcal{M}p$" which merge the Wilson's and Fermat's theorems in a single one.

The function L and the algorithm from §2 will help us to generalize then too, so:

if "a" and m are integers, $m \neq 0$, and $c_1, \ldots c_{\varphi(m)}$ are all residues modulo m relatively prime to m then

$$c_1, \ldots c_{\varphi(m)} a^{\varphi(m_s)+s} - L(o, m) a^s = \mathcal{M}m$$

respectively

$$-L(o, m) a^{\varphi(m_s)+s} + c_1, \ldots c_{\varphi(m)} a^s = \mathcal{M}m$$

or more:

$$(x + c_1) \ldots (x + c_{\varphi(m)}) a^{\varphi(m_s)+s} - L(x, m) a^s = \mathcal{M}m$$

respectively

$$-L(x, m) a^{\varphi(m_s)+s} + (x + c_1) \ldots (x + c_{\varphi(m)}) a^s = \mathcal{M}m$$

which reunite Fermat, Euler, Whilson, Lagrange and Moser (respectively Sierpinski).

3) A partial spreading of Moser's and Sierpinski's results the author also obtained (see [6], probelm 7.140, p.173-174), so: if m is a positive integer, $m \neq 0$, 4, and "a" is an integer, then $(a^m - a)(m-1)! = \mathcal{M}m$, reuniting Fermat and Wilson in other way.

4) Leibniz enuciated that: "if p is prime then $(p-2)! \equiv 1 (\bmod p)''$";

we consider "$c_i < c_{i+1} (\bmod m)$" if $c_i' < c_{i+1}'$ where $0 \leq c_i' < |m|, 0 \leq c_{i+1}' < |m|$ and $c_i \equiv c_i' (\bmod m)$, $c_{i+1} \equiv$ $\equiv c_{i+1}' (\bmod m)$

it sees simply that if $c_1, c_2, \ldots c_{\varphi(m)}$ are all residues modulo m relatively prime to m ($c_i < c_{i+1} (\bmod m)$) for all i, $m \neq 0$) then $c_1 c_2 \ldots c_{\varphi(m)-1} \equiv \pm 1 (\bmod m)$ if $m \in A$ respectively $m \notin A$, because $c_{\varphi(m)} \equiv -1 (\bmod m)$

Bibliography:

[1] Lejeune-Dirichlet, "Vorlesungen über Zahlentheorie", 4te Auflage, Braunschweig 1894, §38.

[2] Sierpinski, Waclaw, "Ce ştim şi ce nu ştim despre numerele prime", Ed. Ştiinţifică, Bucharest, 1966.

[3] Smarandache, Florentin, "O generalizare a teoremei lui Euler referitoare la congruenţă", Bulet. Univ. Braşov, seria C, Vol. XXIII, pp.7-12, 1981;
see Mathematical Reviews: 84J: 10006.

[4] Smarandache, Florentin, "Généralisations et généralités", Ed. Nouvelle, Fès, Morocco, pp.9-13, 1984.

[5] Smarandache, Florentin, "A function in the number theory", An. Univ. Timişoara, seria şt.mat., Vol.XVIII, fasc.1, pp.79-88, 1980;sea M.R.:83c:10008.

[6] Smarandache, Florentin, "Problèmes avec et sans... problèmes!", Somipress, Fès, Morocco, 1983; sea M.R.:84K:00003.

[Published in "Libertas Mathematica", University of Texas, Arlington, Vol. XII, 1992, pp.181-5]

A GENERAL THEOREM FOR THE CHARACTERIZATION OF N PRIME NUMBERS SIMULTANEOUSLY

§1. **ABSTRACT.** This article presents a necessary and sufficient theorem as N numbers, coprime two by two, to be prime simultaneously.

It generalizes V. Popa's theorem [3], as well as I. Cucurezeanu's theorem ([1], p.165), Clement's theorem, S. Patrizio's theorems [2] etc.

Particularly, this General Theorem offers different characterizations for twin primes, for quadruple primes etc.

§2. **INTRODUCTION.** It is evidently the following:

Lemma 1. Let A, B be nonzero integers. Then:

$AB \equiv 0 (\bmod pB) \Leftrightarrow A \equiv 0 (\bmod p) \Leftrightarrow A / p$ is an integer.

Lemma 2. Let $(p,q) \sim 1$, $(a,p) \sim 1$, $(b,q) \sim 1$.

Then:

$A \equiv 0 (\bmod p)$ and $B \equiv 0 (\bmod q) \Leftrightarrow aAq + bBp \equiv \equiv 0 (\bmod pq) \Leftrightarrow aA + bBp / q \equiv 0 (\bmod p)$ $aA / p + bB / q$ is an integer.

Proof:

The first equivalence:

We have $A = K_1 p$ and $B = K_2 q$ with $K_1,\ K_2 \in \mathbf{Z}$ hence $aAq + bBp = (aK_1 + bK_2)pq$.

Reciprocal: $aAq + bBp = Kpq$, with $K \in \mathbf{Z}$ it results that $aAq \equiv 0 (\bmod p)$ and $bBp \equiv 0 (\bmod q)$, but from our assu tion we find $A \equiv 0 (\bmod p)$ and $B \equiv 0 (\bmod q)$

The second and third equivalence results from lemma 1.

By induction we extend this lemma to

Lemma 3. Let $p_1,\dots p_n$ be coprime integers two by two, and let $a_1,\dots,a_n$ be integer numbers such that $(a_i,p_i) \sim 1$ for all i Then:

$$A_1 \equiv 0(\bmod p_1),\dots,A_n \equiv 0(\bmod p_n) \Leftrightarrow$$

$$\Leftrightarrow \sum_{i=1}^{n} a_i A_i \prod_{j \neq i} p_j \equiv 0(\bmod p_1 \dots p_n) \Leftrightarrow$$

$$\Leftrightarrow (P / D) \cdot \sum_{i=1}^{n} (a_i A_i / p_i) \equiv 0(\bmod P / D),$$

where $P = p_1 \dots p_n$ and D is a divisor of $p \Leftrightarrow \sum_{i=1}^{n} a_i A_i / p_i$ is an integer.

§3. From this last lemma we can find immediately a **GENERAL THEOREM:**

Let P_{ij}, $1 \le i \le n$, $1 \le j \le m_i$, be coprime integers two by two, and let $r_1,\dots,r_n$, $a_1,\dots,a_n$ be integer numbers such that a_i be coprime with r_i for all i.

The following conditions are considered:

(i) $p_{i_1},\dots,p_{in_1}$, are simultaneously prime if and only if $c_i \equiv 0(\bmod r_i)$, for all i.

Then:

The numbers p_{ij}, $1 \le i \le n$, $1 \le j \le m_i$, are simultaneously prime if and only if

$$(*) \qquad (R / D) \sum_{i=1}^{n} (a_i c_i / r_i) \equiv 0(\bmod R / D),$$

where $P = \prod_{i=1}^{n} r_i$ and D is a divisor of R.

Remark

Often in the conditions (i) the module r_i is equal to $\prod_{j=1}^{m_i} p_{ij}$,

or to a divisor of it, and in this case the relation of the General Theorem becomes:

$$(P / D)\sum_{i=1}^{n}(a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \equiv 0(\bmod P / D)$$

where

$$P = \prod_{i,j=1}^{n,m_i} p_{ij} \text{ and } D \text{ is a divisor of } P.$$

Corollaries

We easily obtain that our last relation is equivalent with:

$$\sum_{i=1}^{n} a_i c_i (P / \prod_{j=1}^{m_i} p_{ij}) \equiv 0(\bmod P),$$

and

$$\sum_{i=1}^{n}(a_i c_i / \prod_{j=1}^{m_i} p_{ij}) \text{ is an integer,}$$

etc.

The imposed restrictions for the numbers p_{ij} form the General Theorem are very wide, because if there would be two uncoprime distinct numbers, then at least one from these would not be prime, hence the $m_1+\ldots+m_n$ numbers might not be prime.

The General Theorem has many variants in accordance with the assigned values for the parameters $a_1,\ldots,a_n$, and $r_1,\ldots,r_m$, the parameter D, as well as in accordance with the congruences $c_1,\ldots,c_n$ which characterize either a prime number or many other prime numbers simultaneously. We can start from the theorems (conditiond c_i) which characterize a single prime number (see Wilson, Leibnitz, F. Smarandache [4], or Siminov (p is prime if and only if $(p-k)!\ \ (k-1)!-(-1)^k \equiv 0(\bmod p)$,

when $p \geq k \geq 1$; here, it is preferable to take $k = [(p+1)/2]$, where $[x]$ represents the greatest integer number $\leq x$, in order that the number $(p-k)!\ (k-1)!$ be the smallest possibly) for obtaining, by neams of the General Theorem, conditions c'_j, which characterize many prime numbers simultaneously. Afterwards, from the conditions c_i, c'_j, using the General Theorem again, we find new conditions c''_h which characterize prime numbers simultaneously. And this method can be cotinued analogically.

Remarks

Let $m_i = 1$ and c_i represent the Simionov's theorem for all i

(a) If $D = 1$ it results in V. Popa's theorem, which generalizes in the Cucurezeanu's theorem and the last one generalizes in its turn Clement' theorem!

(b) If $D = P / p_2$ and choosing conveniently the parameters a_i, k_i for $i = 1, 2, 3$, it results in S. Patrizio's theorem.

Several EXAMPLES:

1. Let $p_1, p_2, \ldots, p_n$ be positive integers >1, coprime integers two by two, and $1 \leq k_i \leq p_i$ for all i. Then:

$p_1, p_2, \ldots, p_n$ are simultaneously prime if and only if:(T)

$$\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot \prod_{j \neq i} p_j \equiv 0 (\mathrm{mod}\ p_1 p_2 \cdots p_n)$$

or

$$\text{(U)}\ (\sum_{i=1}^{n} \left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i} \right] \cdot \prod_{j \neq i} p_i / (p_{s+1} \cdots p_n) \equiv$$

$\equiv 0(\bmod p_1 \cdots p_s)$

or

(V) $\sum_{i=1}^{n}\left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i}\right] \cdot p_j / p_i \equiv 0(\bmod p_j)$

or

(W) $\sum_{i=1}^{n}\left[(p_i - k_i)!(k_i - 1)! - (-1)^{k_i}\right] \cdot / p_i$ is an integer.

2. Another relation example (using the first theorem form [4]: p is a prime positive integer if and only if $(p-3)! - (p-1)/2 \equiv 0(\bmod p)$

$$\sum_{i=1}^{n}\left[(p_i - 3)! - (p_i - 1)/2\right] \cdot p_1 / p_i \equiv 0(\bmod p_1)$$

3. The odd numbers ... and ... are twin prime if and only if:
$(p-1)!(3p+2) + 2p + 2 \equiv 0(\bmod p(p+2))$
or
$(p-1)!(p-2) - 2 \equiv 0(\bmod p(p+2))$
or
$\left[(p-1)!+1\right]/p + \left[(p-1)!2+1\right]/(p+2)$ is an integer.

These twin prime characterizations differ from Clement's theorem $((p-1)!4 + p + 4 \equiv 0(\bmod p(p+2)))$

4. Let $(p, p+k) \sim 1$ then: p and $p+k$ are prime simultaneously if and only if $(p-1)!(p+k) + (p+k-1)!p + 2p + k \equiv 0(\bmod p(p+k))$, which differs from I. Cucurezeanu's theorem ([1], p.165):
$k.k!\left[(p-1)!+1\right] + \left[K! - (-1)^k\right]p \equiv \equiv 0(\bmod p(p+k))$

5. Look at a characterization of a quadruple of primes for p, $p+2$, $p+6$, $p+8$:
$[(p-1)!+1]/p+[(p-1)!2!+1]/(p+2)+$
$+[(p-1)!6!+1]/(p+6)+[(p-1)!8!+1]/(p+8)$ be an integer.

6. For $p-2$, p, $p+4$ coprime integers two by two, we find the relation: $(p-1)!+p[(p-3)!+1]/(p-2)$ + $+p[(p+3)!+1]/(p+4)\equiv -1(\mathrm{mod}\ p)$, which differ from S. Patrizio's theorem

$$(8[(p+3)!/(p+4)]+4[(p-3)!/(p-2)]\equiv -11(\mathrm{mod}\ p))$$

References

[1] Cucurezeanu, I. - Probleme de aritmetică şi teoria numerelor, Ed. Tehnică, Bucureşti, 1966.
[2] Patrizio, Serafino - Generalizzazione del teorema di Wilson alle terne prime, Enseignement Math., Vol. 22(2), nr. 3-4, pp.175-184, 1976.
[3] Popa, Valeriu - Asupra unor generalizări ale teoremei lui Clement, Studii şi cercetări matematice, vol.24, nr.9,, pp.1435-1440, 1972.
[4] Smarandache, Florentin - Criterii ca un număr natural să fie prim, Gazeta Matematică, nr.2, pp.49-52; 1981; see Mathematical Reviews (USA): 83a: 10007.

[Presented at the 15th American Romanian Academy Annual Convention, wich was held in Montréal, Québec, Canada, from June 14-18, 1990, at the École Polytechnique de Montréal.Published in "Libertas Mathematica", University of Texas, Arlington, Vol.XI, 1991, pp.151-5]

A METHOD TO SOLVE THE DIOPHANTINE EQUATION $ax^2 - by^2 + c = 0$

ABSTRACT

We consider the equation

(1) $ax^2 - by^2 + c = 0$, with $a, b \in \mathbf{N}^*$ and $c \in \mathbf{Z}^*$

It is a generalization of Pell's equation: $x^2 - Dy^2 = 1$. Here, we show that: if the equation has an integer solution and $a \cdot b$ isn't a perfect square, then (1) has an infinitude of integer solutions; in this case we find a closed expression for (x_n, y_n), the general positive integer solution, by an original method. More, we generalize it for for any diophantine equation of second degree and with two unknowns.

INTRODUCTION

If $ab = k^2$ is a perfect square ($k \in \mathbf{N}$) the equation (1) has at most a finite number of integer solutions, because (1) become: (2) $(ax - ky)(ax + ky) = -ac$

If (a, b) dose not divide c, the diophantine equation hasn't solutions.

METHOD TO SOLVE. Suppose (1) has many integer solutions.

Let (x_o, y_o), (x_1, y_1) be the smallest positive integersolutions for (1), with $0 \le x_o < x_1$ We construct the recurrent sequences:

$$(3) \qquad \begin{cases} x_{n+1} = \alpha x_n + \beta y_n \\ y_{n+1} = \gamma x_n + \delta y_n \end{cases}$$

puting the condition (3) verify (1). It results:

$$\begin{cases} a\alpha\beta = b\gamma\delta & (4) \\ a\alpha^2 - b\gamma^2 = a & (5) \\ a\beta^2 - b\delta^2 = -b & (6) \end{cases}$$

having the unknowns $\alpha, \beta, \gamma, \delta$

We pull out $a\alpha^2$ and $a\beta^2$ from (5), respectively (6), and remplace them in (4) at the square; it obtains

$a\delta^2 - b\gamma^2 = a \quad (7)$

We subatract (7) from (5) and find $\alpha = \pm\delta$ (8).

Remplacing (8) in (4) it obtains $\beta = \pm\frac{b}{a}\gamma$ (9).

Afterwards, remplacing (8) in (5), and (9) in (6) it finds the same equation: $a\alpha^2 - b\gamma^2 = a$ (10).

Because we work with positive solutions only, we take

$$\begin{cases} x_{n+1} = \alpha_o x_n + \frac{b}{a}\gamma_o y_n ; \\ y_{n+1} = \gamma_o x_n + \alpha_o y_n \end{cases}$$

where (α_o, γ_o) is the smallest, positive integer solution of (10) such that $\alpha_o\gamma_o \neq 0$ Let $A = \begin{pmatrix} \alpha_o & \frac{b}{a}\gamma_o \\ \gamma_o & \alpha_o \end{pmatrix} \in \mathcal{M}_2(\mathbf{Z})$

Of course, if (x', y') is an integer solution for (1), then $A\begin{pmatrix} x' \\ y' \end{pmatrix}$, $A^{-1}\begin{pmatrix} x' \\ y' \end{pmatrix}$ are another ones – where A^{-1} is the inverse matrix of A, i.e. $A^{-1} \cdot A = A \cdot A^{-1} = I$ (unit matrix). Hence, if (1) has an integer solution it has an infinite ones. (Clearly $A^{-1} \in \mathcal{M}_2(\mathbf{Z})$)

The **general positive integer solution** of the equation (1) is

$$(x'_n, y'_n) = (|x_n|, |y_n|)$$

(GS1) with $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_o \\ y_o \end{pmatrix}$, for all $n \in \mathbf{Z}$,

where by convertion $A^o = I$ and $A^{-k} = A^{-1} \ldots A^{-1}$ of k times.

In problems it is better to write (GS) as

$\begin{pmatrix} x'_n \\ y'_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_o \\ y_o \end{pmatrix}, \quad n \in \mathbf{N}$

(GS2) and $\begin{pmatrix} x''_n \\ y''_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_1 \\ y_1 \end{pmatrix}, \quad n \in \mathbf{N}^*$

We proof, by reductio and absurdum, (GS2) is a general positive integer solution for (1).

Let (u,v) be a positive integer particular solution for (1). If $\exists k_o \in N{:}(u,v) = A^{k_o}\begin{pmatrix} x_o \\ y_o \end{pmatrix}$, or $\exists k_1 \in \mathbf{N}^*{:}(u,v) = A^{k_1}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}$ then $(u,v) \in$ (GS2). Contrary to this, we calculate $(u_{i+1}, v_{i+1}) = A^{-1}\begin{pmatrix} u_i \\ v_i \end{pmatrix}$ for $i = 0, 1, 2, \ldots$ where $u_o = u$, $v_o = v$

Clearly $u_{i+1} < u_i$ for all or i. After a certain rank $x_o < u_{i_o} < x_1$ it finds either $0 < u_{i_o} < x_o$, but that is absurd.

It is clear we can put

(GS3) $\quad \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \cdot \begin{pmatrix} x_o \\ \varepsilon y_o \end{pmatrix}, \qquad n \in \mathbf{N}$, where $\varepsilon = \pm 1$

We shall now transform the general solution (GS3) **in a closed expression.**

Let λ be a real number. Det $(A - \lambda \cdot I) = 0$ involves the solutions $\lambda_{1,2}$ and the proper vectors $V_{1,2}$ (i.e., $Av_i = \lambda_i v_i$, $i \in \{1,2\}$). Note $P = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}^t \in \mathcal{M}_2(\mathbf{R})$

Then $P^{-1}AP = \begin{pmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{pmatrix}$, whence $A^n = P\begin{pmatrix} \lambda_1^n & 0 \\ 0 & \lambda_2^n \end{pmatrix}P^{-1}$, and remplacing it in ($GS_3$) and doing the calculus we find a closed expression for (GS_3).

EXAMPLES

1. For the diophantine equation $2x^2 - 3y^2 = 5$ at obtains

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix}^n \cdot \begin{pmatrix} 2 \\ \varepsilon \end{pmatrix}, \ n \in \mathbb{N}$$

and $\lambda_{1,2} = 5 \pm 2\sqrt{6}$, $v_{1,2} = (\sqrt{6}, \pm 2)$, whence a closed expression for x_n and y_n:

$$\begin{cases} x_n = \dfrac{4+\varepsilon\sqrt{6}}{4}(5+2\sqrt{6})^n + \dfrac{4-\varepsilon\sqrt{6}}{4}(5-2\sqrt{6})^n \\ y_n = \dfrac{3\varepsilon+2\sqrt{6}}{6}(5+2\sqrt{6})^n + \dfrac{3\varepsilon-2\sqrt{6}}{6}(5-2\sqrt{6})^n \end{cases}, \quad \text{for}$$

all $n \in \mathbb{N}$

2. For equation $x^2 - 3y^2 - 4 = 0$ the general solution in positive integer is:

$$\begin{cases} x_n = (2+\sqrt{3})^n + (2-\sqrt{3})^n \\ y_n = \dfrac{1}{\sqrt{3}}\left[(2+\sqrt{3})^n + (2-\sqrt{3})^n\right] \end{cases}$$

for all $n \in \mathbb{N}$, that is (2, 0), (4, 2), (14, 8), (52, 30),...

EXERCICES FOR READER. Solve the diophantine equations:

3. $x^2 - 12y^2 + 3 = 0$

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ \varepsilon \end{pmatrix} = ?, \ n \in \mathbb{N}$]

4. $x^2 - 6y^2 - 10 = 0$.

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 5 & 12 \\ 2 & 5 \end{pmatrix}^n \cdot \begin{pmatrix} 4 \\ \varepsilon \end{pmatrix} = ?,\ n \in \mathbf{N}$]

5. $x^2 - 12y^2 - 9 = 0$

[Remark: $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 7 & 24 \\ 2 & 7 \end{pmatrix}^n \cdot \begin{pmatrix} 3 \\ 0 \end{pmatrix} = ?,\ n \in \mathbf{N}$]

6. $14x^2 - 3y^2 - 18 = 0$

GENERALIZATIONS

If $f(x,y) = 0$ is a diophantine equation of second degree and with two unknowns, by linear transformations it becomes

(12) $ax^2 + by^2 + c = 0$, with $a,b,c \in \mathbf{Z}$.

If $ab \geq 0$ the equation has at most a finite number of integer solutions which can be found by atempts.

It is easier to present an example:

7. The diophantine equation

(13) $9x^2 + 6xy - 13y^2 - 6x - 16y + 20 = 0$

can becomes

(14) $2u^2 - 7v^2 + 45 = 0$, where

(15) $u = 3x + y - 1$ and $v = 2y + 1$

We solve (14). Thus:

(16) $\begin{cases} u_{n+1} = 15u_n + 28v_n \\ v_{n+1} = 8u_n + 15v_n \end{cases}$, $n \in \mathbf{N}$ with $(u_o, v_o) = (3, 3\varepsilon)$

First solution:

By induction we proof that: for all $n \in \mathbf{N}$ we have v_n is odd, and u_n as well as v_n are multiple of 3. Clearly $v_o = 3\varepsilon$, u_o. For $n + 1$we have: $v_{n+1} = 8u_n + 15v_n$ =even+odd=odd, and of course u_{n+1}, v_{n+1} are multiples of 3 because u_n, v_n are multiple of 3, too.

Hence, there exist x_n, y_n in positive integers for all $n \in \mathbf{N}$:

$$(17)\ \begin{cases} x_n = (2u_n - v_n + 3)/6 \\ y_n = (v_n - 1)/2 \end{cases}$$

(from (15)). Now we find the (GS_3) for (14) as closed expression, and by means of (17) it results the general integer solution of the equation (13).

Second solution

Another expression of the (GS_3) for (13) we obtain if we transform (15) as: $u_n = 3x_n + y_n - 1$ and $v_n = 2y_n + 1$, for all $n \in \mathbf{N}$. Whence, using (16) and doing the calculus, it finds

$$(18)\ \begin{cases} x_{n+1} = 11x_n + \dfrac{52}{3}y_n + \dfrac{11}{3} \\ y_{n+1} = 12x_n + 19y_n + 3 \end{cases},\ n \in \mathbf{N},\ \text{with } (x_o, y_o) =$$

(1,1) or (2, –2) (two infinitude of integer solutions).

Let $A = \begin{pmatrix} 11 & 52/3 & 11/3 \\ 12 & 19 & 3 \\ 0 & 0 & 1 \end{pmatrix}$ Then $\begin{pmatrix} x_n \\ y_n \\ 1 \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ or

$\begin{pmatrix} x_n \\ y_n \\ 1 \end{pmatrix} = A^n \begin{pmatrix} 2 \\ -2 \\ 1 \end{pmatrix}$, always $n \in \mathbf{N}$; (19).

From (18) we have always $y_{n+1} \equiv y_n \equiv \ldots \equiv y_o \equiv 1 \pmod 3$, hence always $x_n \in \mathbf{Z}$. Of course, (19) and (17) are equivalent as general integer solution for (13).

[The reader can calculate A^n (by the same method fiable to the start on this note) and find a closed expression for (19).]

More generally:

This method would can be generalized for the diophantine equations

$$(20) \qquad \sum_{i=1}^{n} a_i X_i^2 = b, \text{ will all } a_i, b. \text{ în } \mathbf{Z}$$

If always $a_i a_j \geq 0$, $1 \leq i < j \leq n$, the equation (20) has at most a finite number of integer solution.

Now, we suppose $\exists\ i_o, j_o \in \{1, \ldots, n\}$ for which $a_{i_0} a_{j_0} < 0$ (the equation presents at least a variation of sign). Analogously, for $n \in \mathbf{N}$, we define the recurrent sequences:

$$(21) \qquad x_h^{(n+1)} = \sum_{i=1}^{n} \alpha_{ih} x_i^{(n)}, \quad 1 \leq h \leq n$$

considering $(x_1^0, \ldots, x_n^0)$ the smallest positive integer solution of (20). It remplaces (21) in (20), it identifies the coefficients and it look for the n^2 unknowns α_{ih}, $1 \leq i, h \leq n$. (This calculus is very intricate, but it can be done by means of a computer.) The method goes on similarly, but the calculus becomes more and more intricate - for example to calculate A^n It must a computer, may be.

(The reader will be able to try his force for the diophantine equation $ax^2 + by^2 - cz^2 + d = 0$, with $a, b, c \in \mathbf{N}^*$ and $d \in \mathbf{Z}$)

REFERENCES

M. Bencze, Aplicații ale unor șiruri de recurență în teoria ecuațiilor diofantiene, Gamma (Brașov), XXI-XXII, Anul VII, Nr.4-5, 1985, pp.15-18.

Z.I. Borevich - I.R. Shafarevich, Teora numerelor, EDP, Bucarest, 1985.

A. Kenstam, Contributions to the Theory of the Diophantine Equations $Ax^n - By^n = C$.

G.H. Hardy and E.M. Wright, Introduction to the theory of numbers, Fifth edition, Clarendon Press, Oxford, 1984.

N. Ivășchescu, Rezolvarea ecuațiilor în numere întregi, Lucrare pentru obținerea titlului de profesor gradul 2 (coordonator G.Vraciu), Univ. din Craiova, 1985.

E. Landau, Elementary Number Theory, Celsea, 1955.

Calvin T. Long, Elementary Introduction to Number Theory, D.C.Heath, Boston, 1965.

L.J. Mordell, Diophantine equations, London, Academia Press, 1969.

C. Stanley Ogibvy, John T. Anderson, Excursions in number theory, Oxford University Press, New York, 1966.

W. Sierpinski, Oeuvres choisies, Tome I. Warszawa, 1974-1976.

F. Smarandache, Sur la résolution d'équations du second degré a deux inconnues dans *Z*, in the book Généralizations et généralités, Ed. Nouvelle, Fès, Marocco; MR:85h:00003.

[Published in "Gaceta Matematica", 2ª Serie, Volumen 1, Numero 2, 1988, pp.151-7; Madrid; translated in Spanish by Francisco Bellot Rasado: <<Un metodo de resolucion de la ecuacion diofantica>>.]

SOME STATIONARY SEQUENCES

§ 1. Define a sequence $\{a_n\}$ by $a_1 = a$ and $a_{n+1} = P(a_n)$, where P is a polynomial with real coefficients. For which a values and for which P polynomials will this sequence be constant after a certain rank?

In this note, the author answers for this question refering to F.Lazebnik & Y.Pilipenko's E 3o36 problem from A.M.M., vol.91.No.2/1984.p.140.

An interesting property of functions admiting fixed points is obtained.

§ 2. Because $\{a_n\}$ is constant after a certain rank, it results that $\{a_n\}$ converges. Hence. $(\exists) e \in \mathbf{R}$: $e = P(e)$ that is the equation $P(x) - x = 0$ admits real solutions. Or P admits fixed ponts ($(\exists) x \in \mathbf{R}$: $P(x) = x$).

Let $e_1, \ldots, e_m$ be all real solutions if this equation.

It constructs the recurrent se E, so:

1) $e_1, \ldots, e_m \in E$;

2) if $b \in E$ then all real solutions if the equation $P(x) = b$ belong to E:

3) no anther element belongs to E, then the obtained elements from the rules 1) or 2), appling for a finite number of times these rules.

We prove that this E set, and the A set of the "a" values for which $\{a_n\}$ becomes constant after a certain rank are indistinct.

"$E \subseteq A$"

1) If $a = e_i$, $1 \le i \le m$ then $(\forall) n \in \mathbf{N}^*$ $a_n = e_i =$ constant.

2) If for $a = b$ the sequence $a_1 = b, a_2 = P(b)$ becomes constant after a certain rank, let x_o be a real solution of the equation

$P(x)-b = 0$, the new formed sequence: $a_1' = x_o$, $a_2' = P(x_o) = b$, $a_3' = P(b)$ ... is indistinct after a certain rank with the first one, hence it becomes constant too, having the some limit.

3) **Begining from a certain** rank, all these sequences converge towards the some limit e (that is: they have the some e value from a certain rank) are indistinct, equal to e.

"$A \le E$"

Let "a" be a value such that: $\{a_n\}$ becomes constant (after a certain rank) equal to e. Of course $e \in \{e_1, \dots, e_m\}$ because $e_1, \dots, e_m$ are the single values towards these sequences can tend.

If a $a \in \{e_1, \dots, e_m\}$, then a $a \in E$

Let $a \notin \{e_1, \dots, e_m\}$ be. Then $(\exists) n_o \in N: a_{n_o+1} = P(a_{n_o}) = e$ hence we obtain a appling the rules 1) or 2) a finite number of times, so: because $e \in \{e_1, \dots, e_m\}$ and the equation $P(x) = e$ admits real solutions we find a_{n_o} among the real solutions of this equation: knowing a_{n_o} we find a_{n_o-1} because the equation $P(a_{n_o-1}) = a_{n_o}$ admits real solutions (because $a_{n_o} \in E$ and our method goes on until we find $a_1 = a$ Hence $a \in E$.

Remark. For $P(x) = x^2 - 2$ we obtain the E 3o36 Problem (A.M.M.).

Here, the E set becomes equal to

$$\{\pm 1, 0, \pm 2\} \cup \Big\{\pm\underbrace{\sqrt{2 \pm \sqrt{2 \pm \sqrt{\dots \pm 2}}}}_{n^o \text{ times}}, n \in \mathrm{N}^*\Big\} \cup$$

$$\cup \Big\{\pm\underbrace{\sqrt{2 \pm \sqrt{\dots \sqrt{2 \pm \sqrt{3}}}}}_{n^o \text{ times}}, n \in \mathrm{N}\Big\}.$$

Hence, for all a $a \in E$ the sequence $a_1 = a$, $a_{n+1} = a_n^2 - 2$ becomes constant after a certain rank, and it converges (of course) towards –1 or 2:

$$(\exists) n_o \in \mathrm{N}^* : (\forall) n \geq n_o \qquad a_n = -1$$

or

$$(\exists) n_o \in \mathrm{N}^* : (\forall) n \geq n_o \qquad a_n = 2$$

[Published in "Gamma", Brașov, XXIII, Anul VIII,
No,1, October 1985,pp. 5-6.]

ON CARMICHAËL'S CONJECTURE

Carmichaël's conjecture is the following: "the equation $\varphi(x) = n$ can not have an unique solution, $(\forall) n \in \mathbb{N}$ where φ is the Euler's function". R.K.Guy exposed in [1] some results on it: Carmichaël himself proved that, if n_o does not verify his conjecture, then $n_o > 10^{37}$; V.L. Klee [2] improved to $n_o > 10^{400}$, and P.Masai & A. Valette increased to lo 10^{10000}. C.Pomerance [4] wrought on it,too.

In this paper we prove the equation $\varphi(x) = n$ admits a finite number of solutions, we find the general form of these solutions, also we prove that, if x_o is the unique solution of this equation (for a $n \in \mathbb{N}$), then x_o is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$ (and $x_o > 10^{10000}$ from [3]).

§ 1. Let x_o be a solution of the equation $\varphi(x) = n$. It considers n fixed. We try to construct another solution $y_o \neq x_o$.

The first method:

We decompose $x_o = a \cdot b$ with a, b integers such that $(a,b) \sim 1$; it seeks an $a' \neq a$ such that $\varphi(a') = \varphi(a)$ and $(a',b) \sim 1$; it results $y_o = a' \cdot b$

The second method:

let's $x_o = q_1^{\beta_1} \dots q_r^{\beta_r}$, where all $\beta_i \in \mathbb{N}^*$, and $q_1, \dots, q_r$ are distinct primes two by twos;

we seek an integer q such that $(q, x_o) \sim 1$ and $\varphi(q)$ divides $x_o / (q_1 \dots q_r)$; then $y_o = x_o q / \varphi(q)$.

We see immediately that we can take q as prime,.

The author conjectures that for any integer $x_o \geq 2$ it is

possible to find by means of one of these methods $y_o \neq x_o$ such that $\varphi(y_o) = \varphi(x_o)$

Lemma 1. The equation $\varphi(x) = n$ admits a finite number of solution, $.(\forall) n \in \mathbf{N}$

Proof. The cases $n = 0, 1$ are trivial.

Let n be fixed, $n \geq 2$. Let's $p_1 < p_2 < .. < p_s \leq n+1$ the sequence of prime numbers. If x_o is solution of our (1) equation then x_o has the form $x_o = p_1^{\alpha_1} \dots p_s^{\alpha_s}$, with all $\alpha_i \in \mathbf{N}$. Each α_i is limited, because

$$(\forall) i \in \{1, 2, \dots, s\}, (\exists) a_i \in \mathbf{N}: p_i^{a_i} \geq n$$

Whence $0 \leq \alpha_i \leq a_i + 1$, for all i. Thus, we find a wide limitation for the number of solution: $\prod_{i=1}^{s} (a_i + 2)$

Lemma 2. Any solution of this equation has the form (1) and (2)

$$x_o = n \cdot \left(\frac{p_1}{p_1 - 1}\right)^{\varepsilon_1} \dots \left(\frac{p_s}{p_s - 1}\right)^{\varepsilon_s} \in \mathbf{Z}$$

where, for $1 \leq i \leq s$, we have $\varepsilon_i = 0$ if $\alpha_i = 0$, or $\varepsilon_i = 1$ if $\alpha_i \neq 0$.

Of course, $n = \varphi(x_o) = x_o \left(\frac{p_1}{p_1 - 1}\right)^{\varepsilon_1} \dots \left(\frac{p_s}{p_s - 1}\right)^{\varepsilon_s}$ whence it results the second form of x_o.

From (2) we find another limitation for the number of the solutions: $2^s - 1$ because each ε_i has two values only, and at least one is not equal to zero.

§ 2. We suppose x_o is the unique solution of this equation.

Lemma 3. x_o is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$.

Proof. We apply our second method.

Because $\varphi(0) = \varphi(3)$ and $\varphi(1) = \varphi(2)$ we take $x_o \geq 4$.

If $2 \nmid x_o$ then is $y_o = 2x_o \neq x_o$ such that $\varphi(y_o) = \varphi(x_o)$, hence $2 | x_o$; if $4 \nmid x_o$ then we can take $y_o = x_o / 2$.

If $3 \nmid x_o$ then $y_o = 3x_o / 2$, hence $3 | x_o$; if $9 \nmid x_o$ then $y_o = 2x_o / 3$, hence $9 | x_o$; whence ...$4 \cdot 9 | x_o$.

If $7 \nmid x_o$ then $y_o = 7x_o / 6$, hence $7 | x_o$; if $49 \nmid x_o$ then $y_o = 6x_o / 7$, hence $49 | x_o$; whence $4 \cdot 9 \cdot 49 | x_o$.

If $43 \nmid x_o$ then $y_o = 43x_o / 42$, hence $43 | x_o$; if $43^2 \nmid x_o$ then $y_o = 42x_o / 43$, hence $43^2 | x_o$; whence $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2 | x_o$

Thus $x_o = 2^{\gamma_1} \cdot 3^{\gamma_2} \cdot 7^{\gamma_3} \cdot 43^{\gamma_4} \cdot t$, with all $\gamma_i \geq 2$ and $(t, 2 \cdot 3 \cdot 7 \cdot 43) \sim 1$ and $x_o > 10^{10000}$ because $n_o > 10^{10000}$.

§ 3. Let $\gamma_i \geq 3$ be. If $5 \nmid x_o$ then $5x_o / 4 = y_o$, hence $5 | x_o$; if $25 \nmid x_o$ then $y_o = 4x_o / 5$, whence $25 | x_o$.

We construct the recurrent set M of prime numbers:

a) the elements $2,3,5 \in M$;

b) if the distinct odd elements $e_1, \ldots, e_n \in M$ and $b_m = 1 + 2^m \cdot e_1, \ldots, e_n$ is prime, with $m = 1$ or $m = 2$, then $b_m \in M$;

c) any element belonging to M is obtained by the utilisation (a finite number of times) of the rules a) or b) only.

The author conjectures that M is infinite what solves this case, because it results there is an infinite of primes which divide X_o. That is absurd.

For example 2, 3, 5, 7, 11, 13, 23, 29, 31, 43, 47, 53, 61,... belong to M.

*

The method from § 3 would can to be continued as a tree (for $\gamma_2 \geq 3$ afterwards $\gamma_3 \geq 3$ etc,), but its ramifications are very much...

Bibliography:

[1] R.K.Guy, Monthly unsolved problems 1969-1983. Amer. Math. Monthly, Vol. 90, No. 10/1983, p. 684.

[2] V.L.Klee, Amer. Math Monthly 76? (969), p. 288.

[3] P.Masai & A,Valette, A lower bound for a counter-example to Carmichaël's conjecture, Boll. Unione Mat.Ital, (6) A_1 (1982), pp. 313-316.

[4] C.Pomerance, Math. Reviews: 49:4917.

[Published in "Gamma", XXIV, Anul VIII, No,2, Februry 1986, pp.13-4]

A PROPERTY FOR A COUNTEREXAMPLE TO CARMICHAËL'S CONJECTURE

Carmichaël has conjectured that:
$(\forall)n \in \mathbf{N}$, $(\exists)m \in \mathbf{N}$, with $m \neq n$, for which $\varphi(n) = \varphi(m)$, where φ is Euler's totient function.

There are many papers on it, but the author cites the on by papers which have influenced him, specialy klee 's ones.

Let n be a counterexamle to Carmichaël's conjecture.

Grosswald has proved n is a multiple of 32, Donnelly has pushed the result to a multiple of 2^{14}, and Klee to a multiple of $2^{42} \cdot 3^{47}$, Smarandache has shown n is a multiple of $2^2 \cdot 3^2 \cdot 7^2 \cdot 43^2$. Masai & Valette have bounded $n > 10^{10000}$

In this note we shall extend these results to: n is a multiple of a product of a very large number of primes.

We construct a recurrent set M so that:

a) the elements $2, 3 \in M$;

b) if the distinct elements $2, 3, q_1, \ldots, q_r \in M$ and $p = 1 + 2^a \cdot 3^b \cdot q_1 \ldots q_r$ is a prime, where $a \in \{0,1,2,\ldots,41\}$ and $b \in \{0,1,2,\ldots,46\}$, then $p \in M$; $r \geq 0$;

c) any element belonging to M is obtaiend only by the utilization (a finite number of times) of the rules a) or b).

Of course, all elements from M are primes.

Let n be a multiple of $2^{42} \cdot 3^{47}$;

if $5 \nmid n$ them there exists $a_n m = 5n/4 \neq n$ so that $\varphi(n) = \varphi(m)$; hence $5 | n$; whence $5 \in M$;

if $5^2 \nmid n$ then there exists $a_n m = 4n/5 \neq n$ with our property; hence $5^2 | n$;

analogously, if $7 \nmid n$ use can take $m = 7n/6 \neq n$, hence $7 | n$; if

$7^2 \nmid n$ we can take $m = 6n / 7 \neq n$; whence $7 \in M$ and $7^2 | n$;etc.

The method continues until it isn't possible to add another prime to M, by its cinsruction.

For example, from the 168 primes less than 1000, only 17 ones do not belong to M (namely: 101, 151, 197, 251, 401, 491, 503, 601, 607, 677, 701, 727, 751, 809, 883, 907, 983); all another 151 primes belong to M.

Note $M = \{2,3,p_1,p_2,\dots,p_s,\dots\}$, then n is a multiple of $2^{42} \cdot 3^{47} \cdot p_1^2 \cdot p_2^2 \dots p_s^2 \dots$ Since our example, M contains at least 151 elements, hence $s \geq 149$.

If M is infinite then there exist no counterexample n, whence Carmichaël's conjecture is solved.

(The author conjectures M is infinite.)

By an electronic computer it is possible to find a very large number of primes which divide n using the method of construction of M, and trying reach newprime p if $p-1$ is a product of primes only from M.

References:

R.D. Carmichël, Note on Euler's ϕ function, Bull. Amer. Math. Soc. 28(1922) 109-110.

H. Donnelly(tbp), On a problem concerning Euler's phi-function, Amer. Math. Monthly 80(1973) 1029-1031.

E. Grosswald, Contribution to the theory of Euler's function $\phi(x)$, Bull. Amer. Math. Soc. 79(1973) 337-341

R.K.Guy, Monthly Research Problems 1969-73,Amer. Math. Monthly 80(1973) 1120-1128.

R.K. Guy,Monthy Unsolved Problems 1969-1983,Amer. Math. Monthly 90(1983) 683-690.

R.K.Guy, Unsolved Problems in Number Theory, Springer-Verlag,1981, problem B 39,53.

V.L.Klee, On a conjecture of Carmichaël,Bull. Amer. Math. Soc. 53(1947) 1183-1186.
V.L.Klee, Is there an n for which $\phi(x)$ has a unique solution?, Amer. Math. Monthly 76(1969) 288-289.
P.Masai et A.Valette, A lower bound for a counterexample to Carmichaël's conjecture, Boll. Unione Mat. Ital. (6) A1(1982) 313-316.
F.GH.Smarandache, On Carmichaël's conjecture, Gamma, Braşov, XXIV, Anul VIII,1986.

[Published in „Gamma", XXV, Anul VIII, No.3, June 1986, pp 4-5]

ON DIOPHANTINE EQUATION $X^2 = 2Y^4 - 1$

In his book of unsolved problems Guy informs us that the equation $x^2 = 2y^4 - 1$ has in positive integers the only solutions (1,1) and (239,13); (Ljunggren has shown it by a difficult proof). But Mordell asks a simple proof.

In this note we find other method of solving.

Note $t = y^2$. The general integer solution for $x^2 - 2t^2 + 1 = 0$ is

$$\begin{cases} x_{n+1} = 3x_n + 4t_n \\ t_{n+1} = 2x_n + 3t_n \end{cases}$$

for all $n \in \mathbf{N}$, where $(x_o, y_o) = (1, \varepsilon)$ with $\varepsilon = \pm 1$ (see F. Gh.S.)

or $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}^n \cdot \begin{pmatrix} 1 \\ \varepsilon \end{pmatrix}$, for all $n \in \mathbf{N}$,

where a matrix att fhe power zero is equal to the unit matrix I.

Let $A = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix}$, and $\lambda \in \mathbf{R}$. Then $\det(A - \lambda \cdot I) = 0$ involves $\lambda_{1,2} = 3 \pm \sqrt{2}$, whence if v is a vector of dimension two then: $Av = \lambda_{1,2} \cdot v$ involves

Let $P = \begin{pmatrix} 2 & 2 \\ \sqrt{2} & -\sqrt{2} \end{pmatrix}$ and $D = \begin{pmatrix} 3 + 2\sqrt{2} & 0 \\ 0 & 3 - 2\sqrt{2} \end{pmatrix}$. We have $P^{-1} \cdot A \cdot P = D$,

or $A^n = P \cdot D^n \cdot P^{-1} = \begin{pmatrix} \frac{1}{2}(a+b) & \frac{\sqrt{2}}{2}(a-b) \\ \frac{\sqrt{2}}{4}(a-b) & \frac{1}{2}(a+b) \end{pmatrix}$, where

$a = (3 + 2\sqrt{2})^n$ and $b = (3 - 2\sqrt{2})^n$ Hence, we find:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} \frac{1+\varepsilon\sqrt{2}}{2}(3+2\sqrt{2})^n + \frac{1-\varepsilon\sqrt{2}}{2}(3-2\sqrt{2})^n \\ \frac{2\varepsilon+\sqrt{2}}{4}(3+2\sqrt{2})^n + \frac{2\varepsilon-\sqrt{2}}{4}(3-2\sqrt{2})^n \end{pmatrix}, n \in \mathbb{N}$$

Or $y_n^2 = \frac{2\varepsilon+\sqrt{2}}{4}(3+2\sqrt{2})^n + \frac{2\varepsilon-\sqrt{2}}{4}(3-2\sqrt{2})^n, n \in \mathbb{N}.$

For $n = 0$, $\varepsilon = 1$ it obtains $y_o^2 = 1$ (whence $x_o^2 = 1$), and for $n = 3$, $\varepsilon = 1$ it obtains $y_3^2 = 169$ (whence $x_3 = 239$).

$$(1)\ y_n^2 = \varepsilon \sum_{k=0}^{\left[\frac{n}{2}\right]} \binom{n}{2k} \cdot 3^{n-2k} \cdot 2^{3k} + \sum_{k=0}^{\left[\frac{n-1}{2}\right]} \binom{n}{2k+1} \cdot 3^{n-2k-1} \cdot 2^{3k+1}$$

It must prove still that y_n^2 is a perfect sguare if and omly if $n = 0,3$.

We can use a similar method for the diophantine equation $x^2 = Dy^4 \pm 1$, or more generally: $C \cdot X^{2a} = DY^{2b} + E$, with $a,b \in \mathbb{N}^*$ and $C,D,E \in \mathbb{Z}^*$, noting $X^a = U$, $Y^b = V$ andapplyng the results of F.S., but the relation (1) becomes very intricate.

Bibliography:

J.H.E. Cohn, The diophantine eguation $y^2 = Dx^4 + 1$, Math. Scand. 42 (1978), 180-188,MR 80a:10031.

R.K.Guy, Unsolved Problems in Number Theory, Springer-Verlag, 1981, Problem D6, 84-85.

W.Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo,I,5(1942)# 5,27pp; MR 8,6.

W. Ljunggren, Some remarks on the diophantine equation $x^2 - Dy^4 = 1$ and $x^4 - Dy^2 = 1$, J. London Math. Soc. 41 (1966),542-544; MR 33# 5555.

40

L.J.Mordell, The diophantine equation $y^2 = Dx^4 + 1$, J. London Math. Soc. 39(1964) 161-164; MR 29#65.

F.Smarandache, A Method to solve Diophantine Equations of two unknowns and second degree,„Gaceta Matematica", 2ª Serie, Volumen1, Numero2,1988, pp 151-7; translated in Spanish by Francisco Bellot Rosado.

[Published in "Gamma", anul IX, November 1986, nr.1, p12.]

ON AN ERDÖS'S OPEN PROBLEM

In one of his book ("Analysis...") Mr.Paul Erdös proposed the following problem:

"The interger n is called a barrier for an arithmetic function f if m+f(m) $m + f(m) \leq n$ for all $m < n$ Question: Are there infinitely many barriers for $\varepsilon\nu(n)$, for some $\varepsilon > 0$? Here $\nu(n)$ denotes the number of distinct prime factors of n."

We found some results onit, which do us to conjecture that are o finite number of barriers, for all $\varepsilon > 0$.

Let $R(n)$ be the relation: $m + \varepsilon\nu(m) \leq n$, $\forall\, m < n$.

Lemma 1. If $\varepsilon > 1$ there are two barriers only: $n = 1$ and $n = 2$ (which we name trivial barriers).

Proof. It is clear for $n = 1$ and $n = 2$ because $\nu(0) = \nu(1) = 0$.

Let $n \geq 3$ be. Then, if $m = n - 1$ we have

$m + \varepsilon\nu(m) \geq n - 1 + \varepsilon > n$, absurd.

Lemma 2. There is an infinite of numbers which cannot be barriers for $\varepsilon\nu(n)$, $\forall\, \varepsilon > 0$.

Proof. Let $s, k \in \mathbf{N}^*$ be such that $s \cdot \varepsilon > k$. We construct n of the form $n = p_{i_1}^{\alpha_{i_1}} \ldots p_{i_s}^{\alpha_{i_s}} + k$, where for all j $\alpha_{i_j} \in \mathbf{N}^*$ and p_{i_j} are pozitive distinct primes.

Taking $m = n - k$ we have $m + \varepsilon\nu(m) = n - k + \varepsilon \cdot s > n$

But there exists an infinite of n because the parameters

$\alpha_{i_1}, \ldots, \alpha_{i_s}$ are arbitrary in $\mathbf{N}^*$

and $p_{i_1}, \ldots, p_{i_s}$ are arbitrary positive distinct primes, also there is an infinite of couples (s, k) for an $\varepsilon > 0$, fixed, with the property $s \cdot \varepsilon > k$.

Lemma 3. For all $\varepsilon \in (0,1]$ there are nontrivial barriers for $\varepsilon\nu(n)$.

Proof. Let t be the greatest natural number such that $t\varepsilon \le 1$ (there is always this t).

Let n be from $[3,\dots,p_1 \cdots p_t p_{t+1})$, where $\{p_i\}$ is therequence of the positive prime. Then $1 \le \nu(n) \le t$.

All $n \in [1,\dots,p_1 \cdots p_t p_{t+1}]$ is a barrier, because:

$\forall\ 1 \le k \le n-1$, if $m = n-k$ we have $m + \varepsilon\nu(m) \le$ $\le n - k + \varepsilon \cdot t \le n$.

Hence, there are at least $p_1 \cdots p_t p_{t+1}$ barriers.

Corollar. If $\varepsilon \to 0$ then n (the number of barriers)$\to \infty$

Lemma 4. Let $n \in [1,\dots,p_1 \cdots p_r p_{r+1}]$ and $\varepsilon \in (0,1]$ be. Then: n is a barrier if and only if $R(n)$ is verified for $m \in \{n-1, n-2, \dots, n-r+1\}$.

Proof. It is sufficiently to prove that $R(n)$ is always verified for $m \le n - r$.

Let $m = n - r - u$ be, $u \ge 0$. Then $m + \varepsilon\nu(m) \le n - r -$ $- u + \varepsilon \cdot r \le n$

Conjecture.

We note $I_r \in [p_1 \cdots p_r, \dots, p_1 \cdots p_r p_{r+1})$. Of course $\bigcup_{r \ge 1} I_r =$ $= \mathrm{N} \setminus \{0,1\}$, and $I_{r_1} \cap I_{r_2} = \varnothing$ for $r_1 \ne r_2$.

Let $\mathcal{N}_r(1+t)$ be the number of all numbers n from I_r such that $1 \le \nu(n) \le t$.

We conjecture that there are a finite numbers of barriers for $\varepsilon\nu(n)$, $\forall\ \varepsilon > 0$;

because $\lim\limits_{r \to \infty} \dfrac{\mathcal{N}_r(1+t)}{p_1 \cdots p_{r+1} - p_1 \cdots p_r} = 0$

and the probability (of finding of $r-1$consecutive values for m, which verify the relation $R(n)$)tends to zero.

ON ANOTHER ERDÖS PROBLEM

Paul Erdös has proposed the following problem:

(1) "Is it true that $\lim\limits_{n\to\infty} \max\limits_{m<n}(m + d(m)) - n = \infty$?,

where $d(m)$ represents the number of all positive divisors of m."

We have clearly:

Lemma l. $(\forall) n \in \mathbf{N} \setminus \{0,1,2\}$, $(\exists)! s \in \mathbf{N}^*$, $(\exists)! \alpha_1, \dots, \alpha_s \in \in \mathbf{N}$, $\alpha_s \neq 0$, suck that $n = p_1^{\alpha_1} \cdots p_s^{\alpha_s} + 1$, where $p_1, p_2, \dots$ constitute the increasing requence of all positive primes.

Lemma 2. Let $s \in \mathbf{N}^*$ We define the subesequence $n_s(i) = p_1^{\alpha_1} \cdots p_s^{\alpha_s} + 1$, where $\alpha_1, \dots, \alpha_s$ are arbitrary elements of $\mathbf{N}$, such that $\alpha_s \neq 0$ and $\alpha_1 + \dots + \alpha_s \to \infty$ and we order it such that $n_s(1) < n_s(2) < \dots$ (increasing sequence)

We find an infinite of subsequences $\{n_s(i)\}$, when s traverres $\mathbf{N}^*$, with the properties:

a) $\lim\limits_{i\to\infty} n_s(i) = \infty$ for all $s \in \mathbf{N}^*$.

b) $\left\{n_{s_1}(i), i \in \mathbf{N}^*\right\} \cap \left\{n_{s_2}(j), j \in \mathbf{N}^*\right\} = \varnothing$, for $s_1 \neq s_2$ (distinct subsequences).

c) $\mathbf{N} \setminus \{0,1,2\} = \bigcup\limits_{s \in \mathbf{N}^*} \left\{n_s(i), i \in \mathbf{N}^*\right\}$

Then:

Lemma 3. If in (1) we calculate the limite for each subsequence $\{n_s(i)\}$ we obtain:

$$\lim_{n\to\infty}\left(\max_{m<p_1^{\alpha_1}\cdots p_s^{\alpha_s}}(m+d(m))-p_1^{\alpha_1}\cdots p_s^{\alpha_s}-1\right)\geq$$

$$\geq\lim_{i\to\infty}\left(p_1^{\alpha_1}\ldots p_s^{\alpha_s}+(\alpha_1+1)\ldots(\alpha_s+1)-p_1^{\alpha_1}\ldots p_s^{\alpha_1}-1\right)=$$

$$=\lim_{i\to\infty}((\alpha_1+1)\ldots(\alpha_s+1)-1)>\lim_{i\to\infty}(\alpha_1+\ldots+\alpha_s)=\infty$$

From these lemmas it results a

Theorem. We have $\overline{\lim_{n\to\infty}}\max_{m<n}(m+d(m))-n=\infty$.

References:

P.Erd...s, Some Unconventional Problems in Number Theory, Mathematics Magazine, Vol 57, No,2, March 1979.

P.Erdös, Letter to the Author, 1986:01:12.

[Published in "Gamma", XXV, Anul VIII, No.3 Iunie 1986, p.5]

METHODS FOR SOLVING LETTER SERIES

Letter - series problems occur in many American tests for measuring quantitative ability of supevisory personnel.

They are more difficult than number-series used for measuring mathematical ability because are unusal and complex.

According to the English alfabetic order:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

as well as to the of a given sequence of letters, the question consists of finding of the following letters of the sequence which obey same rules.

For example: let b d f h j ... be a given sequence; find the next two letters in this series,

Of course, they are l n because letters are taken two by two from the alphabet: b ~~c~~ d ~~e~~ f ~~g~~ h ~~i~~ j ~~k~~ l ~~m~~ n.

In order to solve easier letter - series we transform them into number - series, and in this case it's simpler to use some well - known mathematical procedures.

Method I.

Associate to each letter from the alphabet a number in this way:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z.
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Sample: d c i h n m ... becames 4,3; 9,8; 14,13..., whence the next two numbers will be 19, 18 i.e. s r

Method II.

Let $O(\mathcal{L})$ be the order of the letter $\mathcal{L}$ in the above succession. For example $\mathcal{O}$(F)=6, $\mathcal{O}$(S)=19 etc.

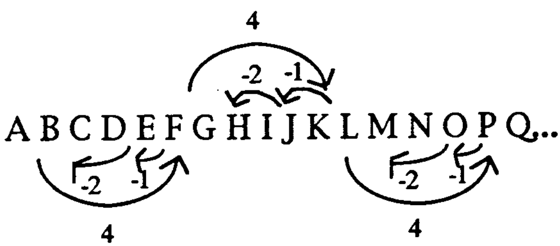
According to the given sequence associate the number zero (0) to its first letter, for the second one the diference between second letter's order and first letter's order,...

We obtain an equivalent number-series.

Sample: bfe c g k j h ... becames $\underline{0}$, 4, –1, –2; $\underline{4}$; 4, –1 –2;...,

whence the next numbers will be: $\underline{4}$; 4, –1, –2; equivalent to l p o m.

See the rule:



Reference:

Passbooks for career opportunities, Computer Aptitude Test (CAT), New York, 1983, National learning Corportion.

GENERALIZATION OF AN ER'S MATRIX METHOD FOR COMPUTING

Er's matrix method for computing Fibronacci numbers and their sums can be extended to the s-additive sequence:

$$g_{-s+1} = g_{-s+2} = \dots = g_{-1} = 0,\ g_o = 1 \text{ and } g_n = \sum_{i=1}^{s} g_{n-i} \text{ for } n>0$$

For example, if we note $S_n = \sum_{j=1}^{n-1} g_j$, we define two $(s+1)\mathrm{x}(s+1)$ matrixes such that:

$$B_n = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 \\ S_n & g_n & g_{n-1} & \cdots & g_{n-s+2} & g_{n-s+1} \\ S_{n-1} & g_{n-1} & g_{n-2} & \cdots & g_{n-s+1} & g_{n-s} \\ \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ S_{n-s+1} & g_{n-s+1} & g_{n-s} & \cdots & g_{n-2s+3} & g_{n-2s+2} \end{bmatrix},$$

$n \geq 1$, and $M = \begin{bmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & 1 & 1 & & 0 \\ \vdots & \vdots & & \ddots & \\ 1 & 1 & 0 & & 1 \\ 1 & 1 & 0 & \dots & 0 \end{bmatrix}$. Thus, we have analogously: $B_{n+1} = M^{n+1}$, $M^{r+c} = M^r \cdot M^c$, whence

$$S_{r+c} = S_r + g_r S_c + g_{r-1} S_{c-1} + \dots + g_{r-s+1} S_{c-s+1},$$

$$g_{r+c} = g_r g_c + g_{r-1} g_{c-1} + \dots + g_{r-s+1} g_{c-s+1},$$ and for $r = c = n$ it results: $S_{2n} = S_n + g_n S_n + g_{n-1} S_{n-1} + \dots + g_{n-s+1} S_{n-s+1}$, $g_{2n} = g_n^2 + g_{n-1}^2 + \dots + g_{n-s+1}^2$; for $r = n$, $c = n-1$ we find:

$$g_{2n-1} = g_n g_{n-1} + g_{n-1} g_{n-2} + \dots + g_{n-s+1} g_{n-s} \text{ etc.}$$

$$S_{2n-1} = S_n + g_n S_{n-1} + g_{n-1} S_{n-2} + \ldots + g_{n-s+1} S_{n-s}$$

Whence we can construct a similar algorithm as M.C.Er for computing s-additive numbers and heir sums.

Reference:

M.C.Er, Fast Computation of Fibonacci Numbers and Their Sums, J. Inf. Optimization Sci. (Delhi), Vol,6 (1985),No.1, pp.41-47.

[Published in "GAMMA", Brașov, Anul X, Nr. 1-2, October 1987, p-8]

ASUPRA TEOREMEI LUI WILSON

& 1. În anul 1770 Wilson găsea următorul rezultat din teoria numerelor "dacă p este prim atunci $(p-1)! \equiv -1 \pmod p$".

V-ați pus vreodată întrebarea ce se întâmplă dacă modulul m nu mai este prim? E simplu, veți răspunde, "dacă m nu este prim și $m \neq 4$ atunci $(m-1)! \equiv 0 \pmod m$" pentru demonstrație vezi [4].

Bine, aș continua eu, dar dacă în produsul din stânga acestei congruențe luăm doar numerele prime cu m?

De aceea vom trata în continuare acest caz, generalizând teorema lui Wilson la un modul oarecare ce ne va conduce la un rezultat frumos.

§ 2. Fie m un număr întreg. Se notează prin $A = \{x \in \mathbf{Z}$, x este de forma $\pm p^n, \pm 2p^n, \pm 2^r$ sau 0, unde p este un număr prim impar și n este număr natural iar r=0, 1 sau 2 $\}$.

Teoremă*. Fie $c_1, c_2, \ldots, c_{\varphi(m)}$ un sistem redus de resturi modulo m. Atunci

$c_1 c_2 \cdots c_{\varphi(m)} \equiv -1 \pmod m$ dacă $m \in A$, respectiv +1 dacă $m \notin A$; unde φ este funcția lui Euler.

Pentru demonstrație vom enunța câteva leme.

Cazurile $m = 0, \pm 1, \pm 2$ se verifică direct, deci le vom înlătura.

Lema 1. $\varphi(m)$ este multiplu de 2.

Lema 2. Dacă $c^2 \equiv 1 \pmod m$ atunci $(m-c)^2 \equiv 1 \pmod m$ și $c(m-c) \equiv -1 \pmod m$ iar $m - c \not\equiv c \pmod m$.

Într-adevăr, dacă $m - c \equiv c \pmod m$ avem că $2c \equiv 0 \pmod m$, adică $(c, m) \neq 1$. Absurd.

Deci am demonstrat că în orice sistem redus de resturi modulo

m există un număr par de elemente c cu proprietatea

$$P_1: \qquad c^2 \equiv 1(\mathrm{mod}\, m).$$

Dacă c_{i_o} este din sistem, cum $(c_{i_o}, m) \cong 1$, rezultă că de asemenea $c_1c_{i_o}, c_2c_{i_o}, \dots, c_{\varphi(m)}c_{i_o}$ constituie un sistem redus de resturi m. Deoarece $(1, m) \cong 1$ rezultă că oricare ar fi c din $c_1, c_2, \dots, c_{\varphi(m)}$ există și este unic un c' din $c_1, c_2, \dots, c_{\varphi(m)}$ astfel încât

$$(1) \qquad cc' \equiv 1(\mathrm{mod}\, m)$$

și reciproc: oricare ar fi c' din $c_1, c_2, \dots, c_{\varphi(m)}$ există și este unic un c din $c_1, c_2, \dots, c_{\varphi(m)}$ astfel încât

$$(2) \qquad c'c \equiv 1(\mathrm{mod}\, m).$$

Prin înmulțirea acestor congruențe pentru toate elementele din sistem și luând una dintre ele în cazul când $c \neq c'$ rezultă că $c_1, c_2, \dots, c_{\varphi(m)} \cdot b \equiv 1(\mathrm{mod}\, m)$, unde b reprezintă produsul tuturor elementelor c pentru care $c' = c$, deoarece în acest caz $c^2 \equiv 1(\mathrm{mod}\, m)$. Aceste elemente care verifică propietatea P_1 se grupează două câte două astfel: c cu $m - c$, și atunci $c(m - c) \equiv -1(\mathrm{mod}\, m)$. Deci

$$c_1, c_2, \dots, c_{\varphi(m)} \equiv \pm 1(\mathrm{mod}\, m),$$

după cum numărul elementelor distinăte c din sistem care au proprietatea P_1 este multiplu de 4 sau nu.

Dacă $m \in A$ ecuația $x^2 \equiv 1(\mathrm{mod}\, m)$ are două soluții (vezi [1], p.83-88), de unde $c_1, c_2, \dots, c_{\varphi(m)} \equiv -1(\mathrm{mod}\, m)$.

Această primă parte a teoremei mai putea fi demonstrată și prin următorul raționament:
dacă $m \in A$ atunci există rădăcini primitive modulo m (vezi [1], p.65-68-72); fie d o astfel de rădăcină; atunci putem reprezenta sistemul redus de resturi modulo m $\left\{c_1, c_2, \dots, c_{\varphi(m)}\right\}$ ca $\left\{d^1, d^2, \dots, d^{\varphi(m)}\right\}$ după rearanjare, de unde $c_1, c_2, \dots, c_{\varphi(m)} \equiv$

$\equiv \left(d^{\frac{\varphi(m)}{2}}\right)^{1+\varphi(m)} \equiv -1(\bmod m)$, deoarece din $d^{\varphi(m)} \equiv$

$\equiv 1(\bmod m)$ avem că $\left(d^{\frac{\varphi(m)}{2}} - 1\right)\left(d^{\frac{\varphi(m)}{2}} + 1\right) \equiv 0(\bmod m)$ deci

$d^{\frac{\varphi(m)}{2}} \equiv -1(\bmod m)$; contrar ar fi implicat că d nu este rădăcină primitivă modulo m.

Pentru a doua parte a demonstrației vom mai enunța alte leme.

Lema 3. Fie numerele întregi nenule, neunitare m_1 și m_2 cu $(m_1, m_2) \cong 1$. Atunci

(3) $x^2 \equiv 1(\bmod m_1)$ admite soluția x_1

și (4) $x^2 \equiv 1(\bmod m_2)$ admite soluția x_2

dacă și numai dacă

(5) $x^2 \equiv 1(\bmod m_1 m_2)$ admite soluția

(5′) $x_3 \equiv (x_2 - x_1)m_1' m_1 + x_1(\bmod m_1 m_2)$,

unde m_1' este inversul lui m_1 față e modulul m_2.

Demonstrație.

Din (3) rezultă $x = m_1 h + x_1$, $h \in \mathbf{Z}$ iar din (4) găsim $x = m_2 k + x_2$, $k \in \mathbf{Z}$ Deci

(6) $m_1 h - m_2 k = x_2 - x_1$

această ecuație diofantică admite soluții întregi deoarece

(7) $(m_1, m_2) \cong 1$

Din (6) rezultă $h \equiv (x_2 - x_1)m_1'(\bmod m_2)$. Astfel $h = (x_2 - x_1)m_1' + m_2 t$, $t \in \mathbf{Z}$ iar $x = (x_2 - x_1)m_1' m_1 + x_1 + m_1 m_2 t$ sau $x \equiv (x_2 - x_1)m_1' m_1 + x_1(\bmod m_1 m_2)$.

(Raționamentul ar fi decurs analog dacă determinam pe k găsind $x \equiv (x_1 - x_2)m_2' m_2 + x_2(\bmod m_1 m_2)$,dar această soluție

este congruentă modulo $m_1 m_2$ cu cea găsită anterior; m'_2 fiind inversul lui m_2 modulo m_1.)

Reciproc. Imediat rezultă că $x_3 \equiv x_1 (\bmod m_1)$ și $x_3 \equiv x_2 (\bmod m_2)$.

Lema 4. Fie x_1, x_2, x_3 soluții pentru congruențele (3), (4) respectiv (5) astfel ca $x_3 \equiv (x_2 - x_1) m'_1 m_1 + x_1 (\bmod m_1 m_2)$

Analog pentru x'_1, x'_2, x'_3.

(O) Vom considera de fiecare dată clasele de resturi modulo m ca având reprezentanți în sistemul 0, 1, 2,..., $|m|-1$.

Atunci dacă $(x_1, x_2) \neq (x'_1, x'_2)$ rezultă că $x_3 \not\equiv x'_3 (\bmod m)$.

Demonstrație prin absurd.

Fie $x_1 \neq x'_1$ (analog se pote arăta dacă $x_2 \neq x'_2$) Din $x_3 \equiv x'_3 (\bmod m_1 m_2)$ ar rezulta și $x_3 \equiv x'_3 (\bmod m_1)$, adică $(x_2 - x_1) m'_1 m_1 + x_1 \equiv (x'_2 - x'_1) m'_1 m_1 + x'_1 (\bmod m_1)$ deci $x_1 \equiv x'_1 (\bmod m_1)$. Cum x_1 și x'_1 sunt din $\{0, 1, 2, \ldots, |m_1| - 1\}$ rezultă $x_1 = x'_1$. Absurd.

Lema 5. Congruența $x^2 \equiv 1 (\bmod m)$ are un număr par de soluții distincte.

Rezultă din Lema 2.

Lema 6. În condițiile Lemei 3 avem că numărul de soluții distincte al congruenței (5) este egal cu produsul dintre numărul soluțiilor congruențelor (3) și (4). Și, toate soluțiile congruenței (5) se obțin din soluțiile congruențelor (3) și (4) prin aplicarea formulei (5').

Într-adevăr din Lemele 3,4 obținem aserțiunea.

Lema 7. Congruența

(8) $x^2 \equiv 1 (\bmod 2^m)$, $n \geq$

are doar patru soluții distincte: $\pm 1, \pm(2^{n-1}-1)$ modulo 2^n.

Prin verificare directă se arată că acestea satisfac (8).

Vom arăta prin inducție că nu mai există și altele.

Pentru $n=3$ se verifică prin încercări, analog pentru $n=4$.

Considerând afirmația adevărată pentru valori $\leq n-1$ să o demonstrăm pentru n.

Menținem observația (O) și remarca următoare:

(9) dacă x_o este soluție pentru congruența (8) ea va fi și pentru congruența $x^2 \equiv 1 (\bmod 2^i)$, $3 \leq i \leq n-1$

Prin absurd fie $a \not\equiv \pm 1, \pm(2^{n-1}-1)$ o soluție pentru (8), Vom arăta că $(\exists) i \in \{3, 4, \ldots, n-1\}$ astfel încât $a^2 \not\equiv 1 (\bmod 2^i)$.

Putem considera $2^{\frac{n}{2}} < a < 2^n - 1$ deoarece a este soluție pentru (8) dacă și numai dacă $-a$ este soluție pentru (8).

Luăm cazul $n = 2k$, $k \geq 2$, întreg. (Se va arăta analog dacă n este impar) Fie $a = 2^k + r$, $1 \leq r \leq 2^{2k} - 2^k - 2$

(10) $a^2 = 2^{2k} + r \cdot 2^{k+1} + r^2 \equiv 1 (\bmod 2^n)$,

de aici $r \neq 1$; rezultă că $r^2 \equiv 1 (\bmod 2^i)$, $3 \leq i \leq k+1$

Din ipoteza de inducție, pentru $k+1$ găsim $r \equiv 2^k - 1 (\bmod 2^{k+1})$ și înlocuind în (10) obținem:

$-2^{k+2} \equiv 0 (\bmod 2^{2k})$, sau $k \leq 2$ deci $n = 4$, Contradicție.

Deci, rezultă valabilitatea lemei,

Lema 8. Congruența $x^2 \equiv 1 (\bmod m)$ are

$$\begin{cases} 2^{s-1}, \text{ dacă } \alpha_1 = 0,1; \\ 2^s, \text{ dacă } \alpha_1 = 2; \\ 2^{s+1}, \text{ dacă } \alpha_1 \geq 3 \end{cases}$$

soluții distincte modulo $m = \varepsilon 2^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, unde $\varepsilon = \pm 1$,

$\alpha_j \in N^*$, $j = 2,3,\ldots,s$ iar p_j sunt numere prime impare diferite două câte două.

Într-adevăr congruența $x^2 \equiv 1(\bmod 2^{\alpha_1})$ are

$$\begin{cases} 1, & \text{dacă } \alpha_1 = 0,1; \\ 2, & \text{dacă } \alpha_1 = 2; \\ 4, & \text{dacă } \alpha_1 \geq 3 \end{cases}$$

soluții distincte, iar congruențele $x^2 \equiv 1(\bmod p_j^{\alpha_j})$, $2 \leq j \leq s$ au fiecare câte două soluții distincte (vezi [1], p.85-88). Din Lema 6 și 7 rezultă și această lemă.

*

Cu aceste leme, rezultă că congruența $c^2 \equiv 1(\bmod m)$, cu $m \notin A$ admite un număr de soluții distincte care este multiplu de 4. De unde $c_1 c_2 \ldots c_{\varphi(m)} \equiv 1(\bmod m)$, rezolvând complet generalizarea teoremei lui Wilson.

Cititorul ar putea generaliza Lemele 2,3,4,5,6,8 și adoptă Lema 7 la cazul în care avem congruența $x^2 \equiv a(\bmod m)$, cu $(a,m) \cong 1$.

Referințe:

[1] Francisco Bellot Rosada, Maria Victoria Deban Miguel, Felix Lopez Fernandez - Asenjo - "Olimpiada Matematica Española/ Problemas propuestos en el distrito Universitario de Valladolid", Universidad de Valladolid, 1992.

[2] "Introduccion a la teoria de numeros primos (Aspectos Algebraicos y Analiticos)", Felix Lopez Fernandez - Asenjo, Juan Tena Ayuso Universidad de Valladolid, 1990.

O METODĂ DE REZOLVARE ÎN NUMERE ÎNTREGI A UNOR ECUAȚII NELINIARE

Considerăm un polinom cu coeficienți întregi, de grad m

$$P(X_1,\dots X_n) = \sum_{\substack{0 \le i_1+\dots+i_n \le m \\ 0 \le i_j \le m,\, j=\overline{1,n}}} a_{i_1\dots i_n} X_1^{i_1}\dots X_n^{i_n}$$

care se poate descompune în factori liniari (ce se pot eventual stabili prin metoda coeficienților nedeterminați):

$$P(X_1,\dots X_n) = \left(A_1^{(1)}X_1+\dots+A_n^{(1)}X_n + A_{n+1}^{(1)}\right)\cdots$$

$$\cdots\left(A_1^{(m)}X_1+\dots+A_n^{(m)}X_n + A_{n+1}^{(m)}\right)+B$$

cu toți $A_j^{(k)}, B$ în $\mathbf{Q}$, dar care prin aducerea la același numitor comun și eliminarea acesteia în ecuația $P(X_1,\dots X_n) = 0$ pot fi considerați întregi. Deci ecuația se transformă în sistemul

$$\begin{cases} A_1^{(1)}X_1+\dots+A_n^{(1)}X_n + A_{n+1}^{(1)} = D_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ A_1^{(m)}X_1+\dots+A_n^{(m)}X_n + A_{n+1}^{(m)} = D_m \end{cases}$$

unde $D_1,\dots,D_m$ sunt divizori ai lui B și $D_1\dots D_m = B$.

Se rezolvă separat fiecare ecuație liniară diofantică și apoi se intersectează soluțiile.

Exemplu. Să se rezolve în numere întregi ecuația:

$$-2x^3+5x^2y+4xy^2-3y^3-3=0$$

Scriem ecuația sub altă formă

$$(x+y)(2x-y)(-x+3y)=3$$

Fie m,n și p divizori ai lui 3, $m\cdot n\cdot p = 3$. Deci

$$\begin{cases} x+y=m \\ 2x-y=n \\ -x+3y=p \end{cases}$$

Pentru ca sistemul să fie compatibil trebuie ca:

$$\begin{vmatrix} 1 & 1 & m \\ 2 & -1 & n \\ -1 & 3 & p \end{vmatrix} = 0, \text{ sau } 5m - 4n - 3p = 0; \quad (1)$$

În acest caz $x = \dfrac{m+n}{3}$ și $y = \dfrac{2m-n}{3}$. (2)

Deoarece $m, n, p \in \mathbf{Z}$, din (1) rezultă – prin rezolvare în numere întregi – că:

$$\begin{cases} m = 3k_1 - k_2 \\ n = \qquad k_2 \\ p = 5k_1 - 3k_2, \quad k_1, k_2 \in \mathbf{Z} \end{cases}$$

care înlocuite în (2) dau $x = k_1$ și $y = 2k_1 - k_2$ Dar $k_2 \in D(3) = \{\pm 1, \ \pm 3\}$. Singura soluție se obține pentru $k_2 = 1$, $k_1 = 0$ de unde $x = 0$ și $y = -1$.

Analog se poate arăta că, de exemplu ecuația:

$$-2x^3 + 5x^2y + 4xy^2 - 3y^3 = 6$$

n-are soluții în numere întregi.

Referințe:

[1] Marius Giurgiu, Cornel Moroti, Florică Puican, Ștefan Smărăndoiu- „Teme și teste de Matematică pentru clasele IV-VIII", Ed. Matex, Rm. Vîlcea, Nr. 3/1991

[2] Ion Nanu, Lucian Tuțescu- „Ecuații Nestandard", Ed. Apollo și Ed. Oltenia, Craiova, 1994.

O GENERALIZARE PRIVIND EXTREMELE UNEI FUNCȚII TRIGONOMETRICE

După lectura pasionantă a acestei cărți [1] (matematică plus literatură!) m-am oprit asupra uneia dintre problemele expuse aici:

La pag. 121, problema 2 cere să se afle maximul expresiei $E(x) = (9+\cos^2 x)(6+\sin^2 x)$. Analog, în G.M. 7/1981, p.280, problema 18820*.

În continuare se dă o generalizare a acestor probleme, și se prezintă o metodă mai simplă de rezolvare. Astfel:

fie $f:\mathbf{R} \to \mathbf{R}$, $f(x) = (a_1 \sin^2 x + b_1)(a_2 \cos^2 x + b_2)$; să se afle valorile extreme ale funcției.

Pentru revolvare, vom ține cont că are loc relația:

$\cos^2 x = 1 - \sin^2 x$, și vom nota $\sin^2 x = y$. Deci $y \in [0,1]$.

Funcția devine: $f(y) = (a_1 y + b_1)(-a_2 y + a_2 + b_2) = -a_1 a_2 y^2 + (a_1 a_2 + a_1 b_2 - a_2 b_1) y + b_1 a_2 + b_1 b_2$, unde $y \in [0,1]$. Deci f este o parabolă.

Dacă $a_1 a_2 = 0$ problema devine banală.

Dacă $a_1 a_2 > 0$, $f(y_{max}) = \dfrac{-\Delta}{4a}$, $y_{max} = \dfrac{-b}{2a}$ (*)

a) când $\dfrac{-b}{2a} \in [0,1]$, valorile căutate sunt cele din (*) Iar

$$y_{min} = \max\left\{-\frac{b}{2a} - 0, 1 + \frac{b}{2a}\right\}$$

b) când $-\dfrac{b}{2a} > 1$, avem $y_{max} = 1$, $y_{min} = 0$.

(evident $f_{max} = f(y_{max})$ și $f_{min} = f(y_{min})$)

c) când $-\dfrac{b}{2a} < 0$, avem $y_{max} = 0$, $y_{min} = 1$.

Dacă $a_1 a_2 < 0$ funcția admite un minim pentru

$$y_{\min} = -\frac{b}{2a},\ f_{\min} \frac{-\Delta}{4a} \text{ (pe axa reală vorbind) } (**)$$

a) când $-\dfrac{b}{2a} \in [0,1]$, valorile căutate sunt cele din (**). Iar

$$y_{\max} = \max\left\{-\frac{b}{2a}, 1 + \frac{b}{2a}\right\}$$

b) când $-\dfrac{b}{2a} > 1$, avem $y_{\max} = 0$, $y_{\min} = 1$.

c) când $-\dfrac{b}{2a} < 0$, avem $y_{\max} = 1$, $y_{\min} = 0$.

Poate cazurile prezentate par complicate și nejustificate, dar reprezentați grafic parabola (sau dreapta) și atunci raționamentele sunt evidente.

Bibliografie:

[1] Viorel Gh. Vodă, „Surprize în matematica elementară", Editura Albatros, București, 1981.

ASUPRA REZOLVĂRII SISTEMELOR OMOGENE

În manualul de algebră de cls. a IX-a (1981), pp 103-104, este prezentată o metodă de rezolvare a sistemelor de două ecuații omogene, cu două necunoscute, de gradul al doilea. În cele ce urmează se descrie o altă metodă de rezolvare.

Fie sistemul omogen:

$$\begin{cases} a_1x^2 + b_1xy + c_1y^2 = d_1 \\ a_2x^2 + b_2xy + c_2y^2 = d_2 \end{cases}$$

cu coeficienți reali.

Se face notația $x = ty$, (sau $y = tx$), care înlocuită în sistem dă:

$$\begin{cases} y^2(a_1t^2 + b_1t + c_1) = d_1 & (1) \\ y^2(a_2t^2 + b_2t + c_2) = d_2 & (2) \end{cases}$$

Împărțind pe (1) la (2) și grupând termenii, rezultă o ecuație de gradul doi în t:

$$(a_1d_2 - a_2d_1)t^2 + (b_1d_2 - b_2d_1)t + (c_1d_2 - c_2d_1) = 0$$

Dacă $\Delta_t < 0$, sistemul nu are soluții.

Dacă $\Delta_t \geq$, sistemul inițial devine echivalent cu sistemele:

$$(S_1) \begin{cases} x = t_1y \\ a_1x^2 + b_1xy + c_1y^2 = d_1 \end{cases}$$

$$\text{și } (S_2) \begin{cases} x = t_2y \\ a_1x^2 + b_1xy + c_1y^2 = d_1 \end{cases}$$

care se rezolvă simplu înlocuind valoarea lui x din prima ecuație în cea de-a doua.

Mai departe se dă o extindere a acestei metode.

Fie sistemul omogen:

$$\sum_{i=0}^{n} a_{i,j}X^{n-i}y^i = b_j,\ j = \overline{1,m}$$

Pentru a-l rezolva, notăm $x = ty$ Rexultă:

$$y^n \sum_{i=0}^{n} a_{i,j} t^{n-i} = b_j,\ j = \overline{1,m}$$

Împărțind pe rând prima ecuație la toate celelalte avem:

$$\left(\sum_{i=0}^{n} a_{i,1} t^{n-i}\right) / \left(\sum_{i=0}^{n} a_{i,j} t^{n-i}\right) = b_1 / b_j,\ j = \overline{2,m}$$

sau:

$$\sum_{i=0}^{n} (a_{i,1} b_j - a_{i,j} b_1) t^{n-i},\ j = \overline{2,m}$$

Se determină valorile $t_1, \ldots, t_p$ reale din acest sistem. Sistemul inițial va fi echivalent cu sistemele:

$$(S_h) \qquad \begin{cases} x = t_h y \\ \sum_{i=0}^{n} a_{i,1} X^{n-1} y^i = b_1 \end{cases}$$

unde $h = \overline{1,p}$.

SUR QUELQUES PROGRESSIONS

Dans cet article on construit des ensembles qui ont la propriété suivante: quel que soit leur partage en deux sous-ensembles, au moins l'un de ces sous-ensembles contient au moins trois éléments en progresssion arithmétique (ou bien géométrique).

Lemme 1: L'ensemble des nombres naturels ne peut pas être partage en deux sous-ensembles ne contenant ni l'un ni l'autre 3 nombres en progression arithmétique.

Supposons le contraire, et soient M_1 et M_2 les deux sous-ensembles. Soit $k \in M_1$

a) Si $k+1 \in M_1$, alors $k-1$ et $k+2$ sont dans M_2, sinon on pourait construire une progression arithmétique dans M_1. Pour la même raison, puisque $k-1$ et $k+2$ sont dans M_2, alors $k-4$ et $k+5$ sont dans M_1. Donc:

$k+1$ et $k+5$ sont dans M_1 donc $k+3$ est dans M_2;

$k-4$ et k sont dans M_1 donc $k+4$ est dans M_1;

on a obtenu que M_2 contient $k+2$, $k+3$ et $k+4$, ce qui est contraire a l'hypothese.

b) si $k+1 \in M_1$ alors $k+1 \in M_2$. Analysons l'élément $k-1$

Si $k-1 \in M_1$, on est dans le cas (a) où deux éléments consécutifs apartiennent au même ensemble.

Si $k-1 \in M_2$. Alors, puisque $k-1$ et $k+1$ sont dans M_2, il en resulte que $k-3$ et $k+3 \in M_2$, donc $\in M_1$. Mais on obtient la progression arithmétique $k-3$, k, $k+3$ dans M_1, contradiction.

Lemme 2: Si on met à part un nombre fini de termes de l'ensemble des entiers naturels, l'ensemble obtenu garde encore la propriété du lemme 1.

Dans le lemme 1, le choix de k était arbitraire, et pour chaque k on obtenait, au moins dans l'un des ensembles M_1 ou M_2 un triplet d'éléments on progression arithmétique: donc au moins un de ces deux ensembles contient une infinité de tels triplets.

Si on met a part un nombre fini de naturels, on met aussi à part un nombre fini de triplets on progression arithmétique. Mais l'un au moins des ensembles M_1 ou M_2 conservera un nombre infini de triplets en progression arithmétique.

Lemme 3 : Si $i_1,...,i_s$ sont des naturels en progression arithmétique, et si $a_1,a_2,...$ est une progression arithmétique (respectivement géométrique), alors $a_{i_1},...,a_{i_s}$ est aussi une progression arithmétique (respectivement géométrigue).

Demostration: pour chaque j on a: $2i_j = i_{j-1} + i_{j+1}$

a) Si $a_1,a_2,...$ est une progression arithmétique de raison r:

$$2a_{i_j} = 2(a_1 + (i_j - 1)r) = (a_1 + (i_{j-1} - 1)r) + (a_1 + (i_{j+1} - 1)r =$$

$$= a_{i_{j-1}} + a_{i_{j+1}}$$

b) Si $a_1,a_2,...$ est une progression géométrique de raison r:

$$(a_{i_j})^2 = \left(a \cdot r^{i_j - 1}\right)^2 = a^2 \cdot r^{2i_j - 2} = \left(a \cdot r^{i_{j-1} - 1}\right) \cdot \left(a \cdot r^{i_{j+1} - 1}\right) =$$

$$= a_{i_{j-1}} \cdot a_{i_{j+1}}$$

Théorème 1: N'importe la manière dont on partage l'ensemble des termes d'une progression arithmétique (respectivement géométrique) en sous-ensembles: dans l'un au moins de ces sous-ensembles il y aura au moins 3 termes en progression arithmétique (respectivement géométrique).

Demostration: D'après le lemme 3, il suffit d'étudier le partage de l'ensemble des indices des termes de la progression en 2 sous-ensembles, et d'analyser l'existence (ou non) d'au moins 3 indices en progression arithmétique dans l'un de ces sous-ensembles.

Mais l'ensemble des indices des termes de la progression est l'ensemble des nombres natureles, et on a démontré au lemme 1 qu'il ne peut pas être partagé en 2 sous-ensembles sans qu'il y ait au moins 3 nombres en progression arithmétique dans l'un de ces sous-ensembles: le théorème est démontré.

Theoreme 2: Un ensemble M qui contient une progression arithmetique (respectivement géométrique) infinie, non constante, conserve la propriété du théorème 1.

En effet, cela découle directement du fait que tout partage de M implique le partage des termes de la progression.

Application: Quelle que soit la façon dont on partage l'ensemble $A = \{1^m, 2^m, 3^m, \ldots\}$ $(m \in \mathbf{R})$ en 2 sous-ensembles, au moins l'un de ces sous-ensembles contient 3 termes en progression géométrique.

(Généralisation du probleme 0:255 de la "Gazeta Matematica", Bucarest, n 10/1981, p 400)

La solution résulte naturellement du théorème 2, si on remarque que A contient la progression géom $a_n = (2^m)^n$, $(n \in \mathbf{N}^*)$.

De plus on peut démontrer que dans l'un au moins des sous-ensembles il y a une infinité de triplets en progression géométrique, parce que A contient une infinité de progressions géométrique différentes: $a_n^{(p)} = (p^m)^n$ avec p premier et $n \in \mathbf{N}^*$, auxquelles on peut appliquer les théorèmes 1 et 2.

SUR LA RESOLUTION DANS L'ENSEMBLE DES NATERELS DES EQUATIONS LINÉAIRES

L'utilité de cet article est qu'il établit si le nombre des solutions naturelles d'une equation linéaire est limité ou non. On expose aussi une méthode de resolution en nombers entiers de l'équation $ax - by = c$ (qui représente une généralisation des lemmes 1 et 2 de [4]), un exemple de résolution d'equation a 3 inconnues, et quelques considération sur la résolution en nombers entiers naturels des équations à n inconnues.

Soit l'équation:

(1) $\sum_{i=1}^{n} a_i x_i = b$ avec tous les a_i, b dans $\mathbf{Z}$, $a_i \neq$et $(a_1,\ldots,a_n)$=ct.

Lemme 1: L'équation (1) admet au moins une solution dans l'ensemble des entiers, si d divise b.

Ce resultat est classique.

Dans (1), on ne nuit pas à la généralité en preant $(a_1,\ldots,a_n)$ =1,parce que dans le cas ou $d \neq 1$ on divise l'équation par ce nombre; si la division n'est pas entière, alors l'équation n'admet pas de solutions naturelles.

I) est evident que chaque équation linéaire homogène admet des solutions dans N: au moins la solution banale!

PEOPRIETES SUR LE NOMBRE DE SOLUTION NATURELLES D'UNE EQUATION LINEAIRE GENERALE.

On va introduire la notion suivante:

Def.1: L'équation (1) a des variations de signe s'il y a au moins deux coefficients a_i, a_j avec $1 \leq i,j \leq n$, tels que $a_i \cdot a_j$

Lemme 2: Une équation (1) qui a des variation de signe admet une infinité de solution naturelles (généralisation du lemme 1 de [4]).

Preuve: De l'hypothèse du lemme résulte que l'équation a h termes positifs non nuls, $1 \leq h \leq n$, et $k = n - h$ termes négatifs non nuls. On a $1 \leq k \leq n$ On suppose que les k premiers termes sont positifs et les k suivants négatifs.

On peut alors écrire:

$$\sum_{t=1}^{h} a_t x_t - \sum_{j=h+1}^{n} a'_j x_j = b \text{ où } a'_j = -a_j > 0.$$

Soit $0 < M = [a_1, \ldots, a_n]$ et $c_i = |M / a_i|$, $i \in \{1,2,\ldots,n\}$

Soit aussi $0 < P = [h,k]$, et $h_1 = P / h$ et $k_1 = P / k$

$$\text{Prenant} \begin{cases} x_t = h_1 c_t \cdot z + x_t^o, & 1 \leq t \leq h \\ x_j = k_1 c_j \cdot z + x_j^o & h+1 \leq j \leq n \end{cases}$$

$$\text{où } z \in \mathbf{N},\ z \geq \max\left\{ \left[\frac{-x_t^o}{h_1 c_t} \right], \left[\frac{x_j^o}{k_1 c_j} \right] \right\} + 1$$

et x_j^o, $i \in \{1,2,\ldots,n\}$ une solution particulière entière (qui existe d'après le lemme 1), on obtient une infinite de de solutions dans l'ensemble des naturels por l'équation (1).

Lemme 3: a) Une équation (1) qui n'a pas dev ariation de signe a au maximum un nombre limité de solutions naturelles.

b) Dans ce cas, pour $b \neq$, constant, l'équation a le nombre maximum de solutions si et seulement si $a_1 = 1$ pour $i \in \{1,2,\ldots,n\}$.

Preuve (voir aussi [6]).

a) On considère tous les $a_i > 0$ o (dans le cas contraire, multiplier l'équation par -1).

Si $b > 0$, il est evident que l'équation n'a aucune solution (dans N).

Si $b = 0$, l'équation admet seulement la solution banale.

Si $b > 0$, alors chaque inconnue x_i prend des valeurs entières positives comprises entre 0 et $b / a_i = d_i$ (fini), et pas nécessairement toutes ces valoeurs. Donc le nombre maximumde solutions est inférieur ou égal à:

$\prod_{i=1}^{n}(1 + d_i)$ qui est fini.

b) Pour $b \neq 0$, constant, $\prod_{i=1}^{n}(1 + d_i)$ est maximum ssi les d_i sont maximums, càd ssi a_i pour tout i de $i = \{1,2,\dots,n\}$

Théorème 1: L'équation (1) admet une infinité de solution naturelles si et seulement si elle a des variation de signe.

Ceci résulte naturellment de ce qui précède.

Méthode de résolution.

Théorème 2: Soit l'équation a coefficients entiers $ax - by = c$, où a et $b > 0$ et (a,b)=1. Alors la solution générale en nombres naturels de cette équation est:

$\begin{cases} x = bk + x_o \\ y = ak + y_o \end{cases}$ où (x_o, y_o) est une solution particulière entiere de l'equation,

et $k \geq \max\{[-x_o / b],[-y_o, a]\}$ est un parametre entier (généralisation du lemme 2 de [4]).

Preuve, II résulte de [1] que la solution générale entière de l'équation est $\begin{cases} x = bk + x_o \\ y = ak + y_o \end{cases}$ où (x_o, y_o) est une solution particulière entière de l'équation et $k \in \mathbf{Z}$. Puisque x et y sont ds entiers naturels, il nous faut imposer des conditions à k, d'où la suite du théorème.

SYSTEMATISONS! Pour résoudre **dans l'ensemble des**

naturels une équation linéaire à n inconnues on utilise les resultate antérieurs de la façon suivante;

a) Si l'équation n'a pas de variation de signe, comme elle a un nombre limité de solution naturelles, la resolution est faite par épreuves (vir aussi [6]

b) Si elle a des variation de signe et que b divisible par d, alors elle admet une infinité de solutions naturelles. On détermine d'abord sa solution générale entière (voir [2], [5]):

$$x_i = \sum_{j=1}^{n-1} \alpha_{ij} k_j + \beta_i,\ 1 \le i \le n \text{ où tous les } \alpha_{ij}, \beta_i \in \mathbf{Z} \text{ et les } k_j$$

sont des paramètres entiers.

En appliquant la restriction $x_i \geq 0$ pour i de $\{1,2,\ldots n\}$, on détermine les conditions qui doivent être réalisées par les paramètres entiers k_j por tout j de $\{1,2,\ldots n-1\}$. (c)

Le cas $n = 2$ et $n = 3$ peut être traité par cette méthode, mais quand n augmente, les conditions (c) deviennent de plus en plus difficiles à trouver.

Eemple: Résoudre dans N l'équation $3x - 7y + 2z = -18$.

Sol.:dans **Z** on obtient la solution générale entière:

$$\begin{cases} x = k_1 \\ y = k_1 + 2k_2 \\ z = 2k_1 + 7k_2 - 9 \end{cases} \quad \text{avec } k_1 \text{ et } k_2 \text{ dans } \mathbf{Z}.$$

Les conditions (c) résultent des inégalités $x \geq 0$, $y \geq 0$, $z \geq 0$. Il en résulte $k_1 \geq$ et aussi $k_2 \geq [-k_1 / 2] + 1$ et $k_2 \geq [(9 - 2k_1)/7] + 1$, c'est-à-dire $k_2 \geq [(2 - 2k_1)/7] + 2$.

Avec ces conditions sur k_1 et k_2 on a la solution générale en nombers naturale de l'équation.

BIBLIOGRAPHIE:

[1] Creangă I., Cazacu C., Mihuț P., Opaiț Gh., Reisher, Corina - "Introducere în teoria numerelor", Editura didactică și pedagogică, București, 1965.

[2] Ion D., Ion, Niță C. - "Elemente de aritmetică cu aplicații în tehnici de calcul", Editura tehnică, Bucarest, 1978.

[3] Popovici C.P. - "Logica și teoria numerelor", Editura didactică și pedagogică, Bucarest, 1970.

[4] Andrica, Dorin și Andreescu, Titu - "Existența unei soluții de bază pentru ecuația "$ax^2 - by^2 = 1$", Gazeta Matematică, nr. 2/1981.

[5] Smarandache, Florentin Gh.- "Un algorithme de résolution des l'ensemble des nombres entiers des équations linéaires", Analele Universității din Craiova, 1981.

[6] Smarandache, Florentin Gh. - Problema E: 6919, G.M. 7/1980.

SUR LA RESOLUTION D'EQUATIONS DU SECOND DEGRÉ A DEUX INCONNUES DANS Z

Propriété 1: L'equation $x^2 - y^2 = c$ admet des solutions entières si et seulement si c appartient à 4Z ou est impair.

Preuve: l'équation $(x-y)(x+y) = c$ admet des solutions dans Z ssi il existe c_1 et c_2 de Z tels que $x - y = c_1$, $x + y = c_2$, et $c_1 c_2 = c$. D'où $x = \frac{c_1 + c_2}{2}$ et $y = \frac{c_2 - c_1}{2}$

Mais x et y sont des entiers ssi $c_1 + c_2 \in 2Z$ c'est-a-dire:

1) ou bien c_1 et c_2 sont impairs, d'où c impar (et réciproquement).

2) ou bien c_1 et c_2 sont pairs, d'où $c \in 4Z$. Réciproquement, si $c \in 4Z$, alors on peut décomposer o en deux facteurs c_1 et c_2 pairs, et tels que $c_1 c_2 = c$.

Remarque 1:

La propriété 1 est vraie aussi pour la résolution dans **N**, puisqu'on peut supposer $c \geq 0$ (dans le cas contraire, on multiplie l'équation par (-1)), et on prend $c_2 \geq c_1 \geq 0$, d'ou $x \geq 0$ et $y \geq 0$.

Propriété 2: L'équation $x^2 - dy^2 = c^2$ (ou d n'est un carré parfait), admet une infinité de solutions dans **N**.

Preuve: soient $x = ck_1$, $k_1 \in \mathbf{N}$ et $y = ck_2$, $k_2 \in \mathbf{N}$, $c \in \mathbf{N}$.

Il en résulte que $k_1^2 - dk_2^2 = 1$ ou l'on reconnaît l'equation de Pell-Fermat, qui admet une infinité de solutions dans **N**, (u_n, v_n). Alors $x_n = cu_n$, $y_n = cv_n$ constituent une infinité de solutions naturelles de notre équation.

Propriété 3: L'equation $ax^2 - by^2 = c$ $(\neq 0)$ où ab $ab = k^2$, $(k \in \mathbf{Z})$, admet un nombre fini de solution naturelles.

Preuve: on peut considérer a,b,c comme des nombres positifs: dans le cas contraire, on multiplie éventuellement l'équation par (-1) et on change le nom des variables. Multiplions l'équation par a, on aura:

$z^2 - t^2 = d$ avec $z = ax \in \mathrm{N}$, $t = ky \in \mathrm{N}$ et $d = ac > 0$. (1)

On resout comme dans la propriete 1, ce qui donne z et t. Mais dans (1) on a un nombre fini de solutions naturelles, parce qu'il existe un nombre fini de diviseurs entiers pour un nombre de $\mathbf{N}^*$. Comme les couples (z,t) sont en nombre limité, bien sur les couples $(z/a, t/k)$ aussi, ainsi que les couples (x, y).

Propriété 4: Si $ax^2 - by^2 = c$, ou $ab \neq k^2$ $(k \in \mathbf{Z})$ admet une solution particulière non triviale dans N, alors elle admet une infinite de solutions dans $\mathbf{N}$.

Preuve: on pose:

$$(2) \begin{cases} x_n = x_o u_n + b y_o v_n \\ y_n = y_o u_n + a x_o v_n \end{cases} \qquad (n \in \mathrm{N})$$

où (x_o, y_o) est la solution particulière naturelle pour l'equation initiale, et $(u_n, v_n)_{n \in \mathrm{N}}$ est la solution générale naturele pour l'équation: $u^2 - abv^2 = 1$, nommée la résolvante Pell, qui admet une infinité de solutions.

Alors $ax_n^2 - by_n^2 = (ax_o^2 - by_o^2)(u_n^2 - abv_n^2) = c$

Donc (2) vérifie l'équation initiale.

CONVERGENCE D'UNE FAMILLE DE SERIES

Dans cet article, on construit une famille d'expressions $\mathcal{E}(n)$.
Pour chaque élément E(n) de $\mathcal{E}(n)$, la convergence de la série $\sum_{n=n_E} E(n)$ pourra être décidée d'après les théorèmes de l'article.
L'article donne assi des applications.

(1) Préliminaire.
Pour rendre l'expression plus aisée, nous utiliserons les fonctions récursives. Quelques notation et notions seront introduites pour simplifier et réduire la matière de cet article.

(2) Definitions: lemmes.
Nous contruisons récursivement une famille d'expressions $\mathcal{E}(n)$.
Pour chaque expression $E(n) \in \mathcal{E}(n)$, le degré de l'expression est défini récursivement et note $d^o E(n)$, et son coefficient dominant est noté $c(E(n))$.

1. Si a est une constante réelle, alors $a \in \mathcal{E}(n)$.
   $d^o a = 0$ et $c(a) = a$
2. L'entier positif $n \in \mathcal{E}(n)$.
   $d^o n = 1$ et $c(n) = 1$.
3, si $E_1(n)$ et $E_2(n)$ appartiennent a $\mathcal{E}(n)$ avec $d^o E_1(n) = r_1$ et $d^o E_2(n) = r_2$, $c(E_1(n)) = a_1$ et $c(E_2(n)) = a_2$, alors:
   a) $E_1(n)E_2(n) \in \mathcal{E}(n)$; $d^o(E_1(n)E_2(n)) = r_1 + r_2$;
   $c(E_1(n)E_2(n))$ vaut $a_1 a_2$.

b) si $E_2(n) \neq 0 \ \ \forall n \in N(n \geq n_{E_2})$, alors $\dfrac{E_1(n)}{E_2(n)} \in \mathcal{E}(n)$ et

$$d^o\left(\frac{E_1(n)}{E_2(n)}\right) = r_1 - r_2,\ c\left(\frac{E_1(n)}{E_2(n)}\right) = \frac{a_1}{a_2}.$$

c) si:

α est un réel constant et si l'operation utilisée a un sens $(E_1(n))^\alpha$ (pr. tt. $n \in \mathrm{N}$, $n \geq n_{E_1}$), alors

$(E_1(n))^\alpha \in \mathcal{E}(n)$, $d^o((E_1(n))^\alpha) = r_1\alpha$, $c((E_1(n))^\alpha) = a_1{}^\alpha$.

d) si $r_1 \neq r_2$ alors $E_1(n) \pm E_2(n) \in \mathcal{E}(n)$,

$d^o(E_1(n) \pm E_2(n))$ est le max de r_1 et r_2, et $c(E_1(n) \pm E_2(n)) = a_1$, respectivement a_2 suivant que le degré est r_1 et r_2.

e) si $r_1 = r_2$ et $a_1 + a_2 \neq 0$, alors $E_1(n) + E_2(n) \in \mathcal{E}(n)$,

$d^o(E_1(n) + E_2(n)) = r_1$ et $c(E_1(n) + E_2(n)) = a_1 + a_2$.

f) si $r_1 = r_2$ et $a_1 - a_2 \neq 0$, alors $E_1(n) - E_2(n) \in \mathcal{E}(n)$,

$d^o(E_1(n) - E_2(n)) = r_1$ et $c(E_1(n) - E_2(n)) = a_1 - a_2$.

4. Toute expression obtenue par application un nombre fini de fois du pas 3 appartient à $\mathcal{E}(n)$

Note l. De la définition de $\mathcal{E}(n)$ il résulte que, si $E(n) \in \mathcal{E}(n)$ alors $c(E(n)) \neq 0$ et que $c(E(n))=0$ si et seulement si $E(n) \equiv 0$.

Lemme l. Si $E(n) \in \mathcal{E}(n)$ et $c(E(n)) > 0$, alors il existe $n' \in \mathrm{N}$, tel que pour tout $n > n'$, $E(n) > 0$.

Preuve: soit $c(E(n)) = a_1 > 0$ et $d^o(E(n)) = r$.

Si $r > 0$, alors $\lim\limits_{n\to\infty} E(n) = \lim\limits_{n\to\infty} n^r \dfrac{E(n)}{n^r} = \lim\limits_{n\to\infty} a_1 n^r = +\infty$

donc il existe $n' \in \mathrm{N}$ tel que, qqst $n \geq n'$ on ait $E(n) > 0$.

Si $r < 0$, alors $\lim\limits_{n\to\infty} \dfrac{1}{E(n)} = \lim\limits_{n\to\infty} \dfrac{n^{-r}}{\dfrac{E(n)}{n^r}} = \dfrac{1}{a_1} \lim\limits_{n\to\infty} n^{-r} = +\infty$

donc il existe $n' \in \mathbf{N}$, tel que pour tout $n \geq n'$, $\frac{1}{E(n)} > 0$ on ait $E(n)>0$.

Si $r = 0$, alors ou bien $E(n)$ est une constante réelle positive, ou bien $\frac{E_1(n)}{E_2(n)} = E(n)$, avec $d^o E_1(n) = d^o E_2(n) = r_1 \neq 0$, d'après ce que nous venons de voir, $c\left(\frac{E_1(n)}{E_2(n)}\right) = \frac{c(E_1(n))}{c(E_2(n))} = c(E(n)) > 0$. Alors:

* ou bien $c(E_1(n)) > 0$ et $c(E_2(n)) > 0$: il en résulte

$$\left.\begin{array}{l}\text{il existe } n_{E1} \in \mathbf{N}, \forall n \in \mathbf{N} \text{ et } n \geq n_{E1}, E_1(n) > 0 \\ \text{il existe } n_{E2} \in \mathbf{N}, \forall n \in \mathbf{N} \text{ et } n \geq n_{E2}, E_2(n) > 0\end{array}\right\} \Rightarrow$$

il existe $n_E = \max(n_{E1}, n_{E2}) \in \mathbf{N}$, $\forall n \in \mathbf{N}$, $n \geq n_E$, $E(n) \frac{E_1(n)}{E_2(n)} > 0$.

* ou bien $c(E_1(n)) < 0$ et $c(E_2(n)) < 0$ et alors: $E(n) = \frac{E_1(n)}{E_2(n)} = \frac{-E_1(n)}{-E_2(n)}$ ce qui nous ramène au cas précédent.

Lemme 2. Si $E(n) \in \mathcal{E}(n)$ et $c(E(n)) < 0$, alors il existe $n' \in \mathbf{N}$, tel que qqst $n > n'$, $E(n) < 0$.

Preuve: l'exoression $-E(n)$ a la propriété que $c(-E(n)) > 0$, d'après la définition récursive. D'après le lemme 1:
il existe $n' \in \mathbf{N}$, $n \geq n'$, $-E(n) > 0$, c'est-à-dire
$+E(n) < 0$, cqfd.

Note 2. Pour prouver le théoreme suivant, nous supposons connu le critère de convergence des séries et certaines proprietes de ces dernières.

(3) Théorème de convergence et applications.

Théorème : soit $E(n) \in \mathcal{E}(n)$ avec $d^o E(n) = r$ soit les séries $\sum\limits_{n \geq n_\varepsilon} E(n)$, $E(n) \not\equiv 0$. Alors:

A) si $r < -1$ la série est absolument convergente.

B) si $r \geq -1$ elle est divergente où $E(n)$ a un sens $\forall n \geq n_E, n \in \mathbb{N}$

Preuve: d'après les lemmes 1 et 2, et parce que:

la série $\sum\limits_{n \geq n_E} E(n)$ converge $\Leftrightarrow$ la série $-\sum\limits_{n \geq n_E} E(n)$ converge,

nous pouvons considérer la série $\sum\limits_{n \geq n_E} E(n)$ comme une série à termes positifs. Nous allons prouver que la série $\sum\limits_{n \geq n_E} E(n)$ a la meme nature que la série $\sum\limits_{n \geq 1} \frac{1}{n^{-r}}$. Appliquons le second critère de comparaison:

$$\underset{n \to \infty}{\text{limite}} \frac{E(n)}{\frac{1}{n^{-r}}} = \underset{n \to \infty}{\text{limite}} \frac{E(n)}{n^r} = c(E(n)) \neq \pm\infty.$$ D'apres la note 1 si $E(n) \not\equiv 0$ alors $c(E(n)) \neq 0$ et donc la serie $\sum\limits_{n \geq n_E} E(n)$ a la même nature que la serie $\sum\limits_{n \geq 1} \frac{1}{n^{-r}}$, c'est-a-dire:

A) si $r < -1$ alors la série est convergente:

B) si $r > -1$ alors la série est divergente.

Pour $r < -1$ la serie est absolment convergente car c'est une série à termes positifs.

Applications: On peut en trouver beaucoup. En voici quelques-unes intéressantes:

Si $P_q(n)$, $R_s(n)$ sont des polynômes en n de degré q, s, et que $P_q(n)$ et $R_s(n)$ appartiennent à $\mathcal{E}(n)$:

1) $\sum_{n\geq n_{PR}} \frac{\sqrt[k]{P_q(n)}}{\sqrt[h]{R_S(n)}}$ est $\begin{cases} \text{convergent} & \text{si } s/h - q/k > 1 \\ \text{divergent} & \text{si } s/h - q/k \leq 1 \end{cases}$

2) $\sum_{n\geq n_R} \frac{1}{R_s(n)}$ est $\begin{cases} \text{convergent}, & \text{si } s > 1 \\ \text{divergent}, & \text{si } s \leq 1 \end{cases}$

Exemple: la serie $\sum_{n\geq 2} \frac{\sqrt[2]{n+1}\cdot\sqrt[3]{n-7}+2}{\sqrt[5]{n^2}-17}$ est divergente parce que $\frac{2}{5}-(1/2+1/3) < 1$ et si on appelle $E(n)$ chaque quotient de cette série, $E(n)$ appartient à $\mathcal{E}(n)$ et a un sens pour $n \geq 2$.

REZOLVAREA CONGRUENȚELOR

În acest articol se determină unele propietăți și metode de rezolvare a congruentelor.

&1 Aplicații la rezolvarea congruențelor liniare

Teorema 1. Congruența liniară $a_1x_1+\ldots+a_nx_n \equiv b(\bmod m)$ are soluții dacă și numai dacă $(a_1,\ldots,a_n,m)|b$.

Demonstrație:

$a_1x_1+\ldots+a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1x_1+\ldots+a_nx_n - my = b$ este ecuație liniară care are soluții în numere întregi $\Leftrightarrow$ $(a_1,\ldots,a_n,-m)|b \Leftrightarrow (a_1,\ldots,a_n,m)|b$.

Dacă $m = 0$, $a_1x_1+\ldots+a_nx_n \equiv b(\bmod 0) \Leftrightarrow a_1x_1+\ldots+ +a_nx_n = b$ are soluții în numere întregi $\Leftrightarrow (a_1,\ldots,a_n)|b \Leftrightarrow$ $(a_1,\ldots,a_n,0)|b$.

Teorema 2. Congruența $ax \equiv b(\bmod m)$, $m \neq 0$, are d soluții distincte.

Demostrația este diferită de cea din cursurile de teoria numerelor: $ax \equiv b(\bmod m) \Leftrightarrow ax - my = b$ are soluții în numere întregi cum $(a,m) = d|b$ rezultă: $a = a_1d$, $m = m_1d$, $b = b_1d$ și $(a_1,m_1) = 1$, $a_1dx - m_1dy = b_1d \Leftrightarrow a_1x - m_1y = b_1$. Deoarece $(a_1,m_1) = 1$ rezultă că soluția generală a acestei ecuații este $\begin{cases} x = m_1k_1 + x_o \\ y = a_1k_1 + y_o \end{cases}$, $k_1 =$ parametru $\in \mathbf{Z}$, unde (x_o,y_o) constituie o soluție particulară în numere întregi a acestei ecuații; $x = m_1k_1 + x_o$, $k_1 \in \mathbf{Z}$, $m_1, x_o \in \mathbf{Z} \Rightarrow x \equiv m_1k_1 + x_o(\bmod m)$. Dăm valori lui k_1 pentru a afla toate soluțiile congruenței.

Evident $k_1 \in \{0,1,2,...,d-1,d,d+1,...,m-1\}$ care constituie un sistem complet de resturi modulo m.

(Deoarece $ax \equiv b(\bmod m) \Leftrightarrow ax \equiv b(\bmod -m)$, am presupus $m > 0$.)

Fie $D = \{0,1,2,...,d-1\}$; $D \subseteq M$, $\forall \alpha \in M$, $\exists \beta \in D$: $\alpha \equiv \beta(\bmod d) | m_1$

(deoarece D constituie un sistem complet de resturi modulo d)

Rezultă $\alpha m_1 = \beta m_1 (\bmod dm_1)$; cum $x_o = x_o(\bmod dm_1)$ rezultă:

$$m_1\alpha + x_o \equiv m_1\beta + x_o(\bmod m)$$

Deci $\forall \alpha \in M$, $\exists \beta \in D$: $m_1\alpha + x_o \equiv m_1\beta + x_o(\bmod m)$; deci $k_1 \in D$.

$\forall \gamma, \delta \in D$ $\gamma \not\equiv \delta(\bmod d) | \cdot m_1 \Rightarrow \gamma m_1 \not\equiv \delta m_1(\bmod dm_1)$; $m_1 \neq 0$

Rezultă $m_1\gamma + x_o \equiv m_1\delta + x_o(\bmod m)$, adică avem exact $\operatorname{card} D = d$ soluții distincte.

Observația 1. Dacă $m = 0$, congruența $ax \equiv b(\bmod 0)$ are o singură soluție dacă $a|b$; în caz contrar n-are soluții.

Demostrație:

$ax \equiv b(\bmod 0) \Leftrightarrow ax = b$ are soluții în numere întregi $\Leftrightarrow a|b$.

Teorema 3. (O generalizare a teoremei anterioare)

Congruența $a_1x_1 + ... + a_nx_n \equiv b(\bmod m)$, $m_1 \neq 0$, cu $(a_1,...,a_n,m) = d|b$ are $d.|m|^{n-1}$ soluții distincte.

Demostrație:

Deoarece $a_1x_1 + ... + a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1x_1 + ... + a_nx_n \equiv b(\bmod -m)$, putem considera $m > 0$.

Demostrația se face prin inducție după n = numărul variabilelor.

Pentru $n = 1$ afirmația este adevărată conform teormei 2.

Presupunem că este adevărată pentru $n-1$. Să demonstrăm că este adevărată pentru n.

Fie congruența cu n variabile $a_1x_1+...+a_nx_n \equiv b(\bmod m)$

$a_1x_1+...+a_{n-1}x_{n-1} \equiv b-a_nx_n(\bmod m)$ Considerând x_n fixat, congruenta $a_1x_1+...+a_{n-1}x_{n-1} \equiv b-a_nx_n(\bmod m)$ este o congruență cu $n-1$ variabile. Pentru a avea soluții trebuie ca $(a_1,...,a_{n-1},m) = \delta | b-a_nx_n \Leftrightarrow b-a_nx_n \equiv 0(\bmod \delta)$.

Deoarece $\delta | m \Rightarrow \frac{m}{\delta} \in \mathbf{Z}$, deci pot înmulți congruența anterioară cu $\frac{m}{\delta}$. Rezultă $\frac{ma_n}{\delta}x_n \equiv \frac{mb}{\delta}(\bmod \delta \cdot \frac{m}{\delta})$ (*) care are $\left(\frac{ma_n}{\delta}, \delta\frac{m}{\delta}\right) = \frac{m}{\delta}(a_n,\delta) = \frac{m}{\delta}(a_n,(a_1,...,a_{n-1},m)) = \frac{m}{\delta}(a_1,...,$ $a_{n-1},a_n,m)) \frac{m}{\delta}\cdot d =$ soluții distincte pentru x_n. Fie x_n^o o soluție particulară a congruentei (*). Rezultă că $a_1x_1+...+a_{n-1}x_{n-1} \equiv b-a_nx_n^o(\bmod m)$ are, conform ipotezei de inducție, $\delta\cdot m^{n-2}$ soluții dinstincte pentru $x_1,...,x_{n-1}$ unde $\delta = (a_1,...,a_{n-1},m)$.

Deci congruenta $a_1x_1+...+a_{n-1}x_{n-1}+a_nx_n \equiv b(\bmod m)$ are $\frac{m}{\delta}\cdot d\cdot\delta\cdot m^{n-2} = d\cdot m^{n-1}$ soluții distincte pentru $x_1,...,x_{n-1}$ și x_n.

METODĂ DE REZOLVARE A CONGRUENȚELOR LINIARE

Fie congruenta $a_1x_1+...+a_nx_n \equiv b(\bmod m)$, $m \neq 0$ $a_i \equiv a_i'(\bmod m)$ și $b \equiv b'(\bmod m)$ cu $0 \le a_i'$, $b \le m-1$ (am făcut ipoteza nerestrictivă $m > 0$). Obținem $a_1x_1+...+a_nx_n \equiv b(\bmod m) \Leftrightarrow a_1'x_1+...+a_n'x_n \equiv b'(\bmod m)$

ecuație liniară care rezolva în $\mathbf{Z}$ are soluția generală:

$$\begin{cases} x_1 = \alpha_{11}k_1 + \ldots + \alpha_{1n}k_n + \gamma_1 \\ \vdots \\ x_n = \alpha_{n1}k_1 + \ldots + \alpha_{nn}k_n + \gamma_n \\ y = \alpha_{n+1,1}k_1 + \ldots + \alpha_{n+1,n}k_n + \gamma_{n+1}; k_j = \text{parametri} \in \mathbf{Z}, j = \overline{1,n} \end{cases}$$

$\alpha_{ij}, \gamma_i \in \mathbf{Z}$, constante, $i = \overline{1,n+1}$, $j = \overline{1,n}$.

Fie $\alpha'_{ij} \equiv \alpha_{ij} (\mathrm{mod}\, m)$ și $\gamma'_i \equiv \gamma_i (\mathrm{mod}\, m)$ cu $0 \le \alpha'_{ij}$, $\gamma' \le m-1$; $i = \overline{1,n+1}$, $j = \overline{1,n}$.

Deci

$$\begin{cases} x_1 \equiv \alpha'_{11}k_1 + \ldots + \alpha'_{1n}k_n + \gamma'_1 (\mathrm{mod}\, m) \\ \vdots \\ x_n \equiv \alpha'_{n1}k_1 + \ldots + \alpha'_{nn}k_n + \gamma'_n (\mathrm{mod}\, m); k_j = \text{parametri} \in \mathbf{Z}, j = \overline{1,n} \end{cases}$$

Fie $(\alpha'_{1j}, \ldots, \alpha'_{nj}, m) = d_j$, $j \in \overline{1,n}$ Să demonstrăm că pentru k_j este suficient să dăm numai valorile 0, 1, 2,..., $\frac{m}{d_j} - 1$;

pentru $k_j = \frac{m}{d_j} - 1 + \beta'$ cu $\beta' \ge 1$ obținem $k_j = \frac{m}{d_j} + \beta$ cu $\beta \ge 0$; $\beta', \beta \in \mathbf{Z}$.

$\alpha'_{ij}k_j = \alpha''_{ij}d_jk_j = \alpha''_{ij}m + \alpha''_{ij}d_j\beta \equiv \alpha''_{ij}d_j\beta (\mathrm{mod}\, m)$; am notat $\alpha'_{ij} = \alpha''_{ij}d_j$ deoarece $d_j | \alpha'_{ij}$. Notez $m = d_jm_j$, $m_j = \frac{m}{d_j}$.

Fie $\eta \in \mathbf{Z}$, $0 \le \eta \le m-1$ astfel încât $\eta \equiv \alpha''_{ij}d_j\beta (\mathrm{mod}\, d_jm_j)$, rezultă $d_j | \eta$.

Deci $\eta = d_j\gamma$ cu $0 \le \gamma \le m_{j-1}$ deoarece avem că $d_j\gamma \equiv \alpha''_{ij}d_j (\mathrm{mod}\, d_jm_j)$ care este echivalentă cu $\gamma \equiv \alpha''_{ij}\beta (\mathrm{mod}\, m_j)$.

Deci $\forall k_j \in \mathrm{N}$, $\exists \gamma \in \{0, 1, 2, \ldots, m_{j-1}\}$: $\alpha'_{ij}k_j \equiv d_j\gamma (\mathrm{mod}\, m)$;

analog dacă parametrul $k_j \in \mathbf{Z}$ Deci k_j ia valori de la 0, 1, 2,... la cel mult $m_j - 1$; $j \in \overline{1,n}$.

Prin această parametrizare pentru fiecare k_j în (**), se obțin soluțiile congruenței liniare. Se înlătură soluțiile care se repetă. Se obțin exact $d.|m|^{n-1}$ soluții distincte.

Exemplu 1. Să se rezolve următoarea congruentă liniară:

$2x + 7y - 6z \equiv -3 \pmod 4$

Soluție. $7 \equiv 3 \pmod 4$, $-6 \equiv 2 \pmod 4$, $-3 \equiv 1 \pmod 4$

Rezultă $2x + 3y + 2z \equiv 1 \pmod 4$; (2,3,2,4)=1|1 deci congruenta are soluții și anume are $1.4^{3-1} = 16$ soluții distincte.

Ecuația $2x + 3y + 2z - 4t = 1$ rezolvată în numere întregi, are soluția generală:

$$\begin{cases} x = 3k_1 - k_2 - 2k_3 - 1 \equiv 3k_1 + 3k_2 + 2k_3 + 3 \pmod 4 \\ y = -2k_1 \qquad\qquad + 1 \equiv 2k_1 \qquad\qquad + 1 \pmod 4 \\ z = \qquad k_2 \qquad\qquad \equiv \qquad k_2 \qquad\qquad \pmod 4 \end{cases}$$

k_j = parametri $\in \mathbf{Z}, j = \overline{1,3}$

(Expresia lui t n-am mai scris-o deoarece nu ne interesează).

Dăm valori parametrilor. k_j ia valori de la 0 la cel mult $m_j - 1$; k_3 ia valori de la 0 la $m_3 - 1 = \frac{m}{d_3} - 1 = \frac{4}{(2,0,0)} - 1 = \frac{4}{2} - -1 = 1$;

$$k_3 = 0 \Rightarrow \begin{pmatrix} x \equiv 3k_1 + 3k_2 + 3 \pmod 4 \\ y \equiv 2k_1 \qquad + 1 \pmod 4 \\ z \equiv \qquad k_2 \qquad \pmod 4 \end{pmatrix};$$

$$k_3 = 1 \Rightarrow \begin{pmatrix} 3k_1 + 3k_2 + 1 \\ 2k_1 \qquad + 1 \\ k_2 \end{pmatrix}$$

k_1 ia valori de la 0 la cel mult.3.

$$k_1 = 0 \Rightarrow \begin{pmatrix} 3k_2+3 \\ 1 \\ k_2 \end{pmatrix}, \begin{pmatrix} 3k_2+1 \\ 1 \\ k_2 \end{pmatrix};\ k_1 = 1 \Rightarrow \begin{pmatrix} 3k_2+2 \\ 3 \\ k_2 \end{pmatrix}, \begin{pmatrix} 3k_2 \\ 3 \\ k_2 \end{pmatrix};$$

pentru $k_1 = 2$ și 3 se obțin aceleași expresii ca pentru $k_1 = 1$ și 0

k_2 ia valori de la 0 la cel mult 3.

$$k_2 = 0 \Rightarrow \begin{pmatrix} 3 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 0 \end{pmatrix};\ k_2 = 2 \Rightarrow \begin{pmatrix} 1 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \\ 2 \end{pmatrix};$$

$$k_2 = 1 \Rightarrow \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 1 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 1 \end{pmatrix};\ k_2 = 3 \Rightarrow \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 3 \\ 3 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ 3 \end{pmatrix};$$

care reprezintă toate soluțiile distincte ale congruenței.

Observația 2. Prin simplificare sau amplificare a congruenței (împărțirea sau înmulțirea cu un număr $\neq 0, 1, -1$) care afectează și modulul, se pierd soluții, respectiv se introduc soluții străine.

Exemplu 2.

1) Congruența $2x - 2y \equiv 6(\bmod 4)$ are soluțiile $\begin{pmatrix} 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix},$
$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 3 \\ 2 \end{pmatrix}, \begin{pmatrix} 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 3 \end{pmatrix};$

2) Dacă am simplifica prin 2 am obține congruența $x - y \equiv 3(\bmod 2)$, care are soluțiile $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}$; deci se pierd soluții.

3) Dacă am amplifica cu 2 am obține congruenta $4x - 4y \equiv 12(\bmod 4)$, care are soluțiile:

$$\binom{3}{0}, \binom{5}{0}, \binom{7}{0}, \binom{1}{0}, \binom{4}{1}, \binom{6}{1}, \binom{0}{1}, \binom{2}{1},$$
$$\binom{5}{2}, \binom{7}{2}, \binom{1}{2}, \binom{3}{2}, \binom{6}{3}, \binom{0}{3}, \binom{2}{3}, \binom{4}{3},$$
$$\binom{7}{4}, \binom{1}{4}, \binom{3}{4}, \binom{5}{4}, \binom{0}{5}, \binom{2}{5}, \binom{4}{5}, \binom{6}{5},$$
$$\binom{1}{6}, \binom{3}{6}, \binom{5}{6}, \binom{7}{6}, \binom{2}{7}, \binom{4}{7}, \binom{6}{7}, \binom{0}{7};$$

deci se introduc soluții străine.

Observația 3. Prin împărțirea sau înmulțirea unei congruențe nu un număr prim cu modulul, fără a împărți sau înmulți modulul, obținem o congruență care are aceleași soluții ca și cea inițială.

Exemplu 3. Congruența $2x+3y \equiv 2(\mathrm{mod}\, 5)$ are aceleași soluții ca și congruența $6x+9y \equiv 6(\mathrm{mod}\, 5)$ și anume:

$$\binom{0}{1}, \binom{2}{1}, \binom{3}{2}, \binom{4}{3}, \binom{0}{4}.$$

§2. APLICAȚII LA REZOLVAREA SISTEMELOR DE CONGRUENȚE LINIARE

În acest paragraf vom obține câteva teoreme interesante referitoare la sistemele de congruențe și apoi o metodă de rezolvare a lor.

Teorema 1. Sistemul de congruențe liniare: (1) $a_{i1}x_1+...+a_{in}x_n \equiv b(\mathrm{mod}\, m_i)$, $i=\overline{1,r}$ are soluții dacă și numai dacă sistemul de ecuații liniare: (2) $a_{i1}x_1+...+a_{in}x_n - m_i y_i = b$, y_i nocunoscute $\in \mathbf{Z}$, $i=\overline{1,r}$ are soluții în numere întregi.

Demonstrația este evidentă.

Observația 1. Din teorema anterioară rezultă că a rezolva sistemul de congruențe (1) este echivalent cu a rezolva în numere întregi sistemul de ecuații liniare (2).

Teorema 2. (O generalizare a teoremei de la pp.20, din[1]). Sistemul de congruențe $a_i x \equiv b_i (\bmod m_i)$, $m_i \neq 0$, $i = \overline{1,r}$ admite soluții dacă și numai dacă: $(a_i, m_i) | b_i$, $i = \overline{1,r}$ și $(a_i m_j, a_j m_i)$ divide pe $a_i b_j - a_j b_i$, $i, j = \overline{1,r}$.

Demonstrație:

$\forall i = \overline{1,r}$, $a_i x \equiv b_i (\bmod m_i)$ $\Leftrightarrow$ $\forall i = \overline{1,r}$, $a_i x = b_i + m_i y_i$, y_i fiind necunoscute $\in \mathbf{Z}$; aceste ecuații diofantice, luate separat, au soluții dacă și numai dacă $(a_i, m_i) | b_i$, $i = \overline{1,r}$.

$\forall i, j = \overline{1,r}$, din: $a_i x = b_i + y_i m_i \big| \cdot a_j$ și $a_j \cdot x = b_j + y_j \cdot m_j \big| a_i$ obținem: $a_i a_j \cdot x = a_j b_i + a_j \cdot m_i y_i = a_i b_j + a_i \cdot m_j y_j$, ecuații diofantice care au soluții dacă și numai dacă $(a_i m_j, a_j m_i) | a_i b_j - a_j b_i$, $i, j = \overline{1,r}$.

Consecință. (Se obține o formă mai simplă pentru teorema de la pp.20 din [1]) Sistemul de congruențe $x \equiv b_i (\bmod m_i)$, $m_i \neq 0$, $i = \overline{1,r}$ are soluții dacă și numai dacă $(m_i, m_j) | b_i - b_j$, $i, j = \overline{1,r}$.

Demonstrație:

Din teorema 2, $a_i = 1$, $\forall i = \overline{1,r}$ și $(1, m_i) = 1 | b_i$, $i = \overline{1,r}$.

METODĂ DE REZOLVARE A SISTEMELOR DE CONGRUENȚE LINIARE

Fie sistemul de congruențe liniare:

(3) $a_{i1}x_1 + \ldots + a_{in}x_n \equiv b (\bmod m_i)$, $i = \overline{1,r}$, rangul matricii

sistemului fiind $r < n$, $a_{ij}, b_i, m_i \in \mathbf{Z}$, $m_i \neq 0$, $i = \overline{1,r}$, $j = \overline{1,n}$
Conform §1 din acest capitol, putem considera:
(*) $0 \leq a_{ij} \leq |m_i| - 1$, $0 \leq b_i \leq |m_i| - 1$, $\forall i = \overline{1,r}$, $j = \overline{1,n}$. Din teorema 1 și observația 1 rezultă că, a rezolva acest sistem de congruențe este echivalent cu a rezolva în numere întregi sistemul de ecuații: (4) $a_{i1}x_1 + \ldots + a_{in}x_n - m_i y_i = b_i$, $i = \overline{1,r}$, rangul sistemului fiind $r < n$. Folosind algoritm din [2], obținem soluția generală a acestui sistem:

$$\begin{cases} x_1 = \alpha_{11}k_1 + \ldots + \alpha_{1n}k_n + \beta_1 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = \alpha_{n1}k_1 + \ldots + \alpha_{nn}k_n + \beta_n \\ y_1 = \alpha_{n+1,1}k_1 + \ldots + \alpha_{n+1,n}k_n + \beta_{n+1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_r = \alpha_{n+r,1}k_1 + \ldots + \alpha_{n+r,n}k_n + \beta_{n+r} \end{cases}$$

$\alpha_{hj}, \beta_h \in \mathbf{Z}$ și k_j-parametri $\in \mathbf{Z}$.

Fie $m = [m_1, \ldots, m_r] > 0$; deoarece variabilele $y_1, \ldots, y_r$ nu ne interesează, reținem doar expresiile lui $x_1, \ldots, x_n$.
Deci: (5) $x_i = \alpha_{i1}k_1 + \ldots + \alpha_{in}k_n + \beta_i$, $i = \overline{1,n}$ și din nou putem presupune că (**) $0 \leq \alpha_{hj} \leq m - 1$, $0 \leq \beta_h \leq m - 1$, $h = \overline{1,n}$, $j = \overline{1,n}$.

Avem: $x_i \equiv \alpha_{i1}k_1 + \ldots + \alpha_{in}k_n + \beta_i \pmod m$, $i = \overline{1,n}$ Evident k_j parcurse cel mult numerele întregi de la 0 la $m-1$. Conform acelorași observații din §1, acest capitol pentru k_j este suficient să dăm numai valorile $0, 1, 2, \ldots, \dfrac{m}{d_j} - 1$ unde $d_j = (\alpha_{1j}, \ldots, \alpha_{nj}, m)$, oricare ar fi $j = \overline{1,n}$ (***). Prin parametrizarea lui $k_1, \ldots, k_n$ în (5) se obțin toate soluțiile sistemului de

congruențe liniare (1); k_j ia cel mult valoriile $0,1,2,...\frac{m}{d_j}-1$; se înlătură soluțiile care se repetă.

Observația 2. Considerațiile (*), (**) și (***) au rolul de a ușura calculul, de a micșora volumul de calcul. Acest algoritm de rezolvare a congruentelor liniare funcționează și fără aceste considerații, dar e mai dificil.

Exemplu. Să se rezolve sistemul de congruențe liniare:

$$(6)\ \begin{cases} 3x+7y-z\equiv 2(\bmod 2) \\ \quad 5y-2z\equiv 1(\bmod 3) \end{cases}$$

Soluție. Sistemul de congruențe liniare (6) este echivalent cu:

$$(7)\ \begin{cases} x+y+z\equiv 0(\bmod 2) \\ \quad 2y+z\equiv 1(\bmod 3) \end{cases}$$

care este echivalent cu sistemul de ecuații liniare:

$$(8)\ \begin{cases} x+y+z-2t_1=0 \\ \quad 2y+z-3t_2=1 \end{cases}$$

x,y,z,t_1,t_2 necunoscute $\in\mathbf{Z}$

Aceasta are soluția generală (vezi [2]):

$$\begin{cases} x=-2k_1+2k_2+3k_3+1 \\ y=k_1-3k_3-1 \\ z=k_1 \\ t_1=k_2 \\ t_2=k_3 \end{cases}$$

unde k_1,k_2,k_3 sunt parametri $\in\mathbf{Z}$.

Valorile lui t_1 și t_2 nu ne interesează; $m=[2,3]=6$. Deci:

$$\begin{cases} x\equiv 4k_1+2k_2+3k_3+1(\bmod 6) \\ y\equiv k_1+3k_3+5(\bmod 6) \\ z\equiv k_1\ (\bmod 6) \end{cases}$$

k_3 ia valori de la 0 la $\dfrac{6}{(3,3,0,6)} - 1 = 1$; k_2 de la 0 la 2; k_1 de la 0 la cel mult 5.

$$k_3 = 0 \Rightarrow \begin{pmatrix} x \equiv 4k_1 + 2k_2 + 1 \pmod 6 \\ y \equiv \ k_1 \qquad\quad + 5 \pmod 6 \\ z \equiv \ k_1 \qquad\qquad \pmod 6 \end{pmatrix};$$

$$k_3 = 1 \Rightarrow \begin{pmatrix} 4k_1 + 2k_2 + 4 \\ k_1 \qquad + 2 \\ k_1 \end{pmatrix};$$

$$k_2 = 0,1,2 \Rightarrow \begin{pmatrix} 4k_1 + 1 \\ k_1 + 5 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 4 \\ k_1 + 2 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 3 \\ k_1 + 5 \\ k_1 \end{pmatrix},$$

$$\begin{pmatrix} 4k_1 \\ k_1 + 2 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 5 \\ k_1 + 5 \\ k_1 \end{pmatrix}, \begin{pmatrix} 4k_1 + 2 \\ k_1 + 2 \\ k_1 \end{pmatrix};$$

$$k_1 = 0,1,2,3,4,5 \Rightarrow$$

$$\begin{pmatrix}1\\5\\0\end{pmatrix}, \begin{pmatrix}4\\2\\0\end{pmatrix}, \begin{pmatrix}3\\5\\0\end{pmatrix}, \begin{pmatrix}0\\2\\0\end{pmatrix}, \begin{pmatrix}5\\5\\0\end{pmatrix}, \begin{pmatrix}2\\2\\0\end{pmatrix}, \begin{pmatrix}5\\0\\1\end{pmatrix}, \begin{pmatrix}2\\3\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\end{pmatrix}, \begin{pmatrix}4\\3\\1\end{pmatrix}, \begin{pmatrix}3\\0\\1\end{pmatrix}, \begin{pmatrix}0\\3\\1\end{pmatrix},$$

$$\begin{pmatrix}3\\1\\2\end{pmatrix}, \begin{pmatrix}0\\4\\2\end{pmatrix}, \begin{pmatrix}5\\1\\2\end{pmatrix}, \begin{pmatrix}2\\4\\2\end{pmatrix}, \begin{pmatrix}1\\1\\2\end{pmatrix}, \begin{pmatrix}4\\4\\2\end{pmatrix}, \begin{pmatrix}1\\2\\3\end{pmatrix}, \begin{pmatrix}4\\5\\3\end{pmatrix}, \begin{pmatrix}3\\2\\3\end{pmatrix}, \begin{pmatrix}0\\5\\3\end{pmatrix}, \begin{pmatrix}5\\2\\3\end{pmatrix}, \begin{pmatrix}2\\5\\3\end{pmatrix},$$

$$\begin{pmatrix}5\\3\\4\end{pmatrix}, \begin{pmatrix}2\\0\\4\end{pmatrix}, \begin{pmatrix}1\\3\\4\end{pmatrix}, \begin{pmatrix}4\\0\\4\end{pmatrix}, \begin{pmatrix}3\\3\\4\end{pmatrix}, \begin{pmatrix}0\\0\\4\end{pmatrix}, \begin{pmatrix}3\\4\\5\end{pmatrix}, \begin{pmatrix}0\\1\\5\end{pmatrix}, \begin{pmatrix}5\\4\\5\end{pmatrix}, \begin{pmatrix}2\\1\\5\end{pmatrix}, \begin{pmatrix}1\\4\\5\end{pmatrix}, \begin{pmatrix}4\\1\\5\end{pmatrix};$$

care constituie cele 36 de soluții distincte ale sistemului de congruențe liniare (6).

Bibliografie:

[1] Constantin P. Popovici, „Curs de teoria numerelor", EDP, București, 1973.

[2] Florentin smarandache, "Integer algorithms to solve linear equations and systems" , Ed. scientifiques Casablanca, 1984

BAZE DE SOLUȚII PENTRU CONGRUENȚE LINIARE

În această lucrare se stabilesc câteva proprietăți legate de soluțiile unei congruențe liniare, baze de soluții pentru o congruență liniară și determinarea celorlalte soluții pornind de la aceste baze.

Această lucrare continuă articolul meu „Asupra congruențelor liniare".

§1 Noțiuni introductive

Definiția 1. (congruență liniară)

Se numește congruență liniară cu n necunoscută o congruență de forma: $a_1x_1+\ldots+a_nx_n \equiv b(\bmod m)$ (1)
unde $a_1,\ldots,a_n,m \in \mathbf{Z}$, $n \geq 1$, iar x_i, $i=\overline{1,n}$ sunt necunoscutele.

Se cunosc următoarele teorme:

Teorema 1. Congruența liniară (1) are soluții dacă și numai dacă $(a_1,\ldots,a_n,m,b)|b$.

Teorema 2. Congruența liniară (1), dacă are soluții, atunci: $|d|\cdot|m|^{n-1}$ este numărul soluțiilor sale distincte.

(vezi articolul „Asupra congruențelor liniare")

Definiția 2. Două soluții $X=(x_1,\ldots,x_n)$ și $Y=(y_1,\ldots,y_n)$ ale congruenței liniare (1) sunt distincte (diferite) dacă $\exists i \in \overline{1,n}$ astfel $x_i \not\equiv y_i(\bmod m)$

§ 2. Definiții și propietăți asupra congruențelor.

Vom da câteva proprietăți aritmetice care se vor folosi mai departe.

Lema 1. Dacă $a_1,\ldots,a_n \in \mathbf{Z}$, $m \in \mathbf{Z}$ atunci:

$$\frac{(a_1,\ldots,a_n,m)\cdot m^{n-1}}{(a_1,m)\cdot\ldots\cdot(a_n,m)} \in \mathbf{Z}$$

Demonstrația se face prin inducție completă după $n \in \mathbf{N}^*$.

Când $n=1$ este evident.

Presupunând adevărat pentru valori mai mici sau egale cu n, să arătăm pentru $n+1$.

Notăm $x=(a_1,\ldots,a_n)$. Atunci:

$(a_1,\ldots,a_n,a_{n+1},m)\cdot m^n = \left[(x,a_{n+1},m)\cdot m^{2-1}\right]\cdot m^{n-1}$ care se divide conform ipotezei de inducție la $\left[(x,m)\cdot(a_{n+1},m)\right]\cdot m^{n-1} =$ $= \left[(a_1,\ldots,a_n,m)\cdot(a_{n+1},m)\right]\cdot m^{n-1} = \left[(a_1,\ldots,a_n,m)\cdot m^{n-1}\right]\cdot$ $\cdot(a_{n+1},m)$ care se divide tot conform ipotezei de inducție la $\left[(a_1,m)\cdot\ldots\cdot(a_n,m)\right]\cdot(a_{n+1},m) = (a_1,m)\cdot\ldots\cdot(a_n,m)\cdot(a_{n+1},m)$.

Teorema 3. Dacă X^o constituie o soluție (particulară) a congruenței liniare (1) $p=\prod_{i=1}^{n}(a_i,m)$, atunci:

$$X_i \equiv x_i^o + \frac{m}{(a_i,m)}t_i,\ 0 \le t_i < (a_i,m),\ t_i \in \mathbf{N} \quad (*)$$

(i luând valori de la 1 la n) constituie p soluții dinstincte ale lui (1)

Demostrație:

Deoarece modulul congruenței (n) se subînțelege l-am omis, și îl vom omite.

$\sum_1^n a_i x_i = \sum_{i=1}^n a_i x_i^o + \sum_1^n \frac{a_i m}{(a_i,m)}t_i \equiv b+0$ Deci sunt soluții. Să arătăm că sunt și distincte.

$x_i^o + \frac{m}{(a_i,m)}\alpha \not\equiv x_i^o + \frac{m}{(a_i,m)}\beta$ pentru $\alpha,\beta \in \mathbf{N}$, $\alpha \ne \beta$ și

și $0 \leq \alpha,\beta < (a_i,m)$, deoarece mulțimea:

$\left\{ \frac{m}{(a_i,m)} t_i \middle| 0 \leq t_i < (a_i,m), t_i \in \mathbf{N} \right\} \subseteq \{0,1,\dots,n-1\}$ care constituie un sistem complet resturi modulo m, iar $\frac{m}{(a_i,m)}\alpha \neq \frac{m}{(a_i,m)}\beta$ pentru α și β anterior definiții.

Și teorema e terminată.

*

* *

Se consideră Z-modulul A generat de vectori V_i, unde $V_i^* = (\underbrace{0,\dots 0}_{\text{i-1 ori}}, \frac{m}{(a_i,m)}, \underbrace{0,\dots,0}_{\text{n-i ori}})$, $i = \overline{1,n}$, din $\mathbf{Z}^n$. Modulul A are rangul n ($n \geq 1$). Se mai scrie $A = \{v_1,\dots,v_n\}$.

Se introduc câtiva termeni noi.

Definiția 3. Două soluții (vectori soluție) X și Y ale congruenței (1) se numesc independente dacă $X - Y \notin A$

În caz contrar se numesc soluții dependente.

Observația 1. Cu alte cuvinte, dacă X este o soluție a congruenței (1), atunci soluția Y a aceleiași congruențe este independentă cu ea, dacă nu se obține din X prin aplicarea formulei (*) pentru anumite valori ale parametrilor $t_1,\dots,t_n$.

Definiția 4. Soluțiile $X^1,\dots,X^n$ se numesc independente (între ele) dacă ele sunt independente două câte două.

În caz contrac se numesc soluții dependente (între ele).

Definiția 5. Soluțiile $X^1,\dots,X^n$ ale congruenței (1) constituie o bază pentru această congruență, dacă $X^1,\dots,X^n$ sunt indepen-

dente între ele și cu ajutorul lor se pot obține toate soluțiile (distincte) ale congruenței prin procedeul (*) parametrizând pe $t_1, \dots t_n$.

Câteva proprietăți ale soluțiilor congruențelor liniare

1) Dacă soluției X^1 este independentă cu soluția X^2 atunci și X^2 este independentă cu X^1 (comutativitatea relației de „independență").

2) X^1 nu este independență cu X^1.

3) Dacă X^1 este independență cu X^2, X^2 independentă cu X^3 nu implică X^1 independentă cu X^3 (relația nu e tranzitivă).

4) Dacă X este independență cu Y, atunci X este independență cu Y.

Într-adevăr, dacă Y, este dependentă cu Y, atunci $X - Y_1 =$
$= \underbrace{(X-Y)}_{\notin A} + \underbrace{(Y-Y_1)}_{\in A} = Z$. Dacă $Z \in A$, rezultă $(X - Y) =$
$= Z - (Y - Y_1) \in A$ deoarece A este un Z-modul. Absurd.

*

* *

Teorema 4. Notând $P_1 = (a_1, \dots, a_n, m) \cdot |m|^{n-1}$ și $P_2 = (a_1, m) \cdot \ldots \cdot (a_n, m)$ atunci congruența liniară (1) are baza formată din: $\dfrac{P_1}{P_2}$ soluții

Demostrație:

$P_1 > 0$ și $P_2 > 0$ din lema 1 avem $\dfrac{P_1}{P_2} \in \mathbb{N}^*$, deci are sens teorema (considerăm c.m.m.d.c. ca număr pozitiv)

P_1 reprezintă numărul de soluții distincte (în total) al congruenței (1), conform teoremei 2.

P_2 reprezintă numărul de soluții distincte obținute pentru congruența (1) prin aplicarea procedeului (*) (dând toate valorile posibile parametrilor $t_1,\dots,t_n$) unei singure soluții particulare.

Deci trebuie să aplicăm de $\frac{P_1}{P_2}$ ori procedeul (*) pentru a obține toate soluțiile congruenței, adică este nevoie de exact $\frac{P_1}{P_2}$ soluții particulare independente ale congruenței. Adică baza are $\frac{P_1}{P_2}$ soluții.

Observația 2. Orice bază de soluții (pentru o aceeași congruență liniară) are aceeași număr de vectori.

§ 3. Metodă de rezolvare a congruențelor liniare.

Acest paragraf își propune să valorifice rezultatele obținute mai înainte.

Fie congruența liniară (1) cu $(a_1,\dots,a_n,m) = d|b$, $m \neq 0$.

- se determină numărul soluțiilor distincte ale congruenței: $P_1 = |d|\cdot|m|^{n-1}$

- se determină numărul soluțiilor din bază: $S = \dfrac{P_1}{\prod_{i=1}^{n}(a_i,m)}$;

- se construiește Z-modulul $A=\{V_1,\dots,V_n\}$, unde $V_i^t = (\underbrace{0,\dots,0}_{i-1},\frac{m}{(a_i,m)},\underbrace{0,\dots,0}_{n-i})$, $i=\overline{1,n}$.

- se caută s soluții independente (particulare) ale congruenței

- se aplică procedeul (*) astfel:

dacă X^j , $j=\overline{1,s}$ sunt cele s soluții independente din bază,

rezultă că $X^{j(t_1,\dots,t_n)} = \left(x_i^j + \frac{m}{(a_i,m)}t_i\right)\ i=\overline{1,n}$ (*)

sunt toate cele P_1 soluții ale congruenței liniare (1),

$$j=\overline{1,s},\ t_1\times\ldots\times t_n \in \{0,1,2,\ldots,d_1-1\}\times\ldots\times\{0,1,2,\ldots,d_n-1\}$$

unde $d_i = |(a_i,m)|$, $i=\overline{1,n}$.

Observația 3. Corectitudinea acestei metode rezultă din paragrafele anterioare.

Aplicație. Fie congruența liniară neomogenă $2x-6y \equiv 2 \pmod{12}$. Ea are $(2,6,12)\cdot 12^{2-1}=24$ soluții distincte. Baza va avea 24: $[(2,12)\cdot(6,12)]=2$ soluții.

$V_1^t=(6,0)$, $V_2^t=(0,2)$ și $A=\{V_1,V_2\} = \left\{(6t_1,2t_2)^t \mid t_1,t_2 \in \mathbf{Z}\right\}$.

Soluțiile $x\equiv 7 \pmod{12}$ și $y\equiv 4 \pmod{12}$, $x\equiv 1$ și $y\equiv 0$ sunt dependente deoarece $\begin{pmatrix}7\\0\end{pmatrix}-\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}6\\4\end{pmatrix}=1\begin{pmatrix}6\\0\end{pmatrix}+2\begin{pmatrix}0\\2\end{pmatrix}\in A$.

Dar $\begin{pmatrix}4\\1\end{pmatrix}$ este independentă cu $\begin{pmatrix}0\\1\end{pmatrix}$ deoarece $\begin{pmatrix}4\\1\end{pmatrix}-\begin{pmatrix}0\\1\end{pmatrix}\notin A$.

Deci cele 24 soluții ale congruenței se obțin din:

$$\begin{cases} x\equiv 1+6t_1, & 0\le t_1<2,\ t_1\in\mathbf{N}\\ y\equiv 0+2t_2, & 0\le t_2<6,\ t_2\in\mathbf{N}\end{cases}$$

și

$$\begin{cases} x\equiv 4+6t_1, & 0\le t_1<2,\ t_1\in\mathbf{N}\\ y\equiv 1+2t_2, & 0\le t_2<6,\ t_2\in\mathbf{N}\end{cases}$$

prin parametrizarea $(t_1,t_2)\in\{0,1\}\times\{0,1,2,3,4,5\}$.

$$\begin{cases} x\equiv 1+6t_1\\ y\equiv 0+2t_2\end{cases} \Rightarrow \begin{pmatrix}1\\0\end{pmatrix},\begin{pmatrix}1\\2\end{pmatrix},\begin{pmatrix}1\\4\end{pmatrix},\begin{pmatrix}1\\6\end{pmatrix},\begin{pmatrix}1\\8\end{pmatrix},\begin{pmatrix}1\\10\end{pmatrix},$$

$$\begin{pmatrix}7\\0\end{pmatrix},\begin{pmatrix}7\\2\end{pmatrix},\begin{pmatrix}7\\4\end{pmatrix},\begin{pmatrix}7\\6\end{pmatrix},\begin{pmatrix}7\\8\end{pmatrix},\begin{pmatrix}7\\10\end{pmatrix}.$$

$$\begin{cases} x \equiv 4 + 6t_1 \\ y \equiv 1 + 2t_2 \end{cases} \Rightarrow \begin{pmatrix}4\\1\end{pmatrix}, \begin{pmatrix}4\\3\end{pmatrix}, \begin{pmatrix}4\\5\end{pmatrix}, \begin{pmatrix}4\\7\end{pmatrix}, \begin{pmatrix}4\\9\end{pmatrix}, \begin{pmatrix}4\\11\end{pmatrix},$$

$$\begin{pmatrix}10\\1\end{pmatrix}, \begin{pmatrix}10\\3\end{pmatrix}, \begin{pmatrix}10\\5\end{pmatrix}, \begin{pmatrix}10\\7\end{pmatrix}, \begin{pmatrix}10\\9\end{pmatrix}, \begin{pmatrix}10\\11\end{pmatrix};$$

care constituie toate cele 24 soluții distincte ale congruenței date; $\begin{pmatrix}1\\0\end{pmatrix}$ înseamnă: $x \equiv 1 \pmod{12}$ și $y \equiv 0 \pmod{12}$; etc.

Biblografie.

[1] C.P.Popovici – „Teoria numerelor“, Editura didactică și pedagogică, București, 1973.

[2] F.Gh. Smarandache – „Rezolvarea ecuațiilor și a sistemelor de ecuații liniare în numere întregi “, Lucrare de licență, Universitatea din Craiova , 1979.

[Publicat în „ Bulet. Univ. Brașov“, seria C, vol XXII, pp 25-31, 1980 și în „ Bulet st. și tehn. al Instit. Polit«Traian Vuia» Timișoara“, fascicolul 2, tomul 26(40), pp 13-6; MR: 83c: 10024]

CRITERII CA UN NUMĂR NATURAL SĂ FIE PRIM

În acest articol se prezintă câteva condiții neceare și suficiente ca un număr natural să fie prim.

Teorema 1. Fie p un număr natural ≥ 3: p este prim dacă și numai dacă $(p-3)! \equiv \frac{p-1}{2} (\bmod p)$

Demonstrație:

Necesitatea: p este prim $\Rightarrow$ $(p-1)! \equiv -1 (\bmod p)$ conform teoremei lui Wilson. Rezultă $(p-1)(p-2)(p-3)! \equiv$ $\equiv -1(\bmod p)$, sau $2(p-3)! \equiv p-1(\bmod p)$. Dar p fiind număr prim ≥ 3 rezultă ă $(2,p)=1$ și $\frac{p-1}{2} \in \mathbf{Z}$ Are sens împărțirea congruenței cu 2 și obținem concluzia.

Suficiența: Congruența $(p-3)! \equiv \frac{p-1}{2} (\bmod p)$ o înmulțim cu $(p-1)(p-2) \equiv 2(\bmod p)$ (vezi [1], pg.10-16) și rezultă $(p-1)! \equiv -1(\bmod p)$, din teorema lui Wilson, trăgându-se concluzia că p este prim.

Lema 1. Fie m un număr natural >4, Atunci : m nu este număr prim dacă și numai dacă $(m-1)! \equiv 0(\bmod m)$.

Demonstrație:

Suficiența este evientă conform teoremei lui Wilson.

Necesitatea: m se scrie $m = a_1^{\alpha_1} \ldots a_s^{\alpha_s}$, unde a_i sunt numere prime pozitive, distincte două câte două și $\alpha_i \in \mathbf{N}^*$, oricare ar fi i, $1 \leq i \leq s$.

Dacă $s \neq 11$ atunci $a_i^{\alpha_i} < m$, oricare ar fi i, $1 \leq i \leq s$.

Deci $a_1^{\alpha_1} \dots a_s^{\alpha_s}$ sunt factori distincți în produsul $(m-1)!$ deci $(m-1)! \equiv 0 (\bmod m)$.

Dacă $s=1$ atunci $m = a^\alpha$ cu $\alpha \geq 2$ (deoarece m este neprim). Când $\alpha = 2$ avem $a < m$ și $2a < m$ deoarece $m > 4$. Rezultă că a și $2a$ sunt factori diferiți în (m-1)! și deci $(m-1)!$ și deci $(m-1)! \equiv 0(\bmod m)$. Când $\alpha > 2$, avem a<m și $a < m$ și $a^{\alpha-1} < m$, iar a și $a^{\alpha-1}$ sunt factori diferiți în produsul $(m-1)!$.

Deci $(m-1)! \equiv 0(\bmod m)$ și lema e demonstrată în toate cazurile.

Teorema 2. Fie p un număr natura >4. Atunci: p este prim dacă și numai dacă $(p-4)! \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p)$.

Demonstrație:

Necesitatea: $(p-4)!(p-3)(p-2)(p-1) \equiv -1(\bmod p)$ din teorema lui Wilson, sau $6(p-4)! \equiv 1(\bmod p)$; p fiind prim și mai mare decât 4, rezultă că $(6, p) = 1$.

Rezultă că $p = 6k \pm 1$, $k \in \mathbb{N}^*$

A) Dacă $p = 6k-1$, atunci $6 | (p+1)$ și $(6,p)=1$, și împărțind congruența $6(p-4)! \equiv p+1(\bmod p)$, care este echivalentă cu cea inițială, prin 6 obținem:

$$(p-4)! \equiv \frac{p+1}{6} \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p).$$

B) Dacă $p = 6k + 1$, atunci $6 | (1-p)$ și $(6,p)=1$, și împărțind congruența $6(p-4)! \equiv 1-p(\bmod p)$, care este echivalentă cu cea inițială, prin 6 rezultă:

$$(p-4)! \equiv \frac{1-p}{6} \equiv -k \equiv (-1)^{\left[\frac{p}{3}\right]+1} \cdot \left[\frac{p+1}{6}\right] (\bmod p)$$

Suficiența: Trebuie să arătăm că p este prim. Mai întâi arătăm că $p \neq \mathcal{M}6$

Presupunem prin absurd, că $p = 6k$, $k \in \mathbb{N}^*$. Înlocuind în congruența din ipoteză, rezultă $(6k-4)! \equiv -k(\bmod 6k)$. Din inegalitatea $6k-5 \geq k$ pentru $k \in \mathbb{N}^*$, rezultă $k|(6k-5)!$. Din $2|(6k-4)$, rezultă $2k|(6k-5)!(6k-4)$. Deci $2k|(6k-4)!$ și $2k|6k$, rezultă (conform proprietății congruențelor) (vezi [1], pg.9-26) că $2k|(-k)$, ceea ce nu este adevărat și astfel $p \neq \mathcal{M}6$.

Din $(p-1)(p-2)(p-3) \equiv -6(\bmod p)$ prin înmulțire cu congruența inițială rezultă: $(p-1)! \equiv (-1)^{\left[\frac{p}{3}\right]} 6 \cdot \left[\frac{p+1}{6}\right](\bmod p)$.

Considerăm lema 1, pentru $p > 4$ avem:

$$(p-1)! \equiv \begin{cases} 0(\bmod p), & \text{dacă } p \text{ nu este prim;} \\ -1(\bmod p), & \text{dacă } p \text{ este prim;} \end{cases}$$

a) Dacă $p = 6k+2 \Rightarrow (p-1)! \equiv 6k \not\equiv 0(\bmod p)$.

b) Dacă $p = 6k+3 \Rightarrow (p-1)! \equiv -6k \not\equiv 0(\bmod p)$

c) Dacă p=6k +4, $\Rightarrow (p-1)! \equiv -6k \not\equiv 0(\bmod p)$

Deci $p \neq \mathcal{M}6+r$ cu $r \in \{0,2,3,4\}$.

Rezultă că p este de forma: $p = 6k \pm 1$, $k \in \mathbb{N}^*$ și atunci avem: $(p-1)! \equiv -1(\bmod p)$, adică p este prim.

Teorema 3. Dacă p este un număr natural ≥ 5, atunci; p este prim dacă și numai dacă $(p-5)! \equiv rh + \frac{r^2-1}{24}(\bmod p)$, unde $h = \left[\frac{p}{24}\right]$ iar $r = p - 24h$.

Demonstrație:

Necesitatea: p este prim, rezultă $(p-5)!(p-4)(p-3)(p-2)(p-1) \equiv -1(\bmod p)$ sau

$24(p-5)! \equiv -1 (\mathrm{mod}\, p)$.

Dar p se scrie $p = 24h + r$, cu $r \in \{1,5,7,11,13,17,19,23\}$ deoareceeste prim. Se verifică simplu că $\frac{r^2-1}{24} \in \mathbf{Z}$.

$24(p-5)! \equiv -1 + r(24h+r) \equiv 24rh + r^2 - 1 (\mathrm{mod}\, p)$

Cum $24, p = 1$ și $24 | (r^2-1)$ putem împărți congruența cu 24, obținând: $(p-5)! \equiv rh + \frac{r^2-1}{24} (\mathrm{mod}\, p)$

Suficiența: p se poate scrie $p = 24h + r$, $0 \le r < 24$, $h \in \mathrm{N}$. Înmulțind congruența $(p-4)(p-3)(p-2)(p-1) \equiv 24 (\mathrm{mod}\, p)$ cu cea inițială, obținem:

$(p-1)! \equiv r(24h+r) - 1 \equiv -1 (\mathrm{mod}\, p)$

Teorema 4. Fie $p = (k-1)!h + 1$, $k > 2$ și cu număr natural. Atunci: p este prim dacă și numai dacă

$$(p-k)! \equiv (-1)^{h + \left[\frac{p}{h}\right] + 1} \cdot h (\mathrm{mod}\, p).$$

Demonstrație: $(p-1)! \equiv -1 (\mathrm{mod}\, p) \Leftrightarrow (p-k)!(-1)^{k-1}$

$(p-k)!(k-1)! \equiv (-1)^k (\mathrm{mod}\, p)$

Avem: $((k-1)!, p) = 1$. (1)

A) $p = (k-1)!h - 1$.

a) k este număr par $\Rightarrow$ $(p-k)!(k-1)! \equiv 1 + p (\mathrm{mod}\, p)$ (mod p) și, deoarece are loc relația (1) iar $(k-1)! | (1+p)$, prin împărțire cu $(k-1)!$ avem: $(p-k)! \equiv h (\mathrm{mod}\, p)$.

b) k este număr impar $\Rightarrow$ $(p-k)!(k-1)! \equiv -1 - p (\mathrm{mod}\, p)$ și deoarece are loc relația (1) iar $(k-1)! | (-1-p)$, prin împărțirea cu $(k-1)!$ avem: $(p-k)! \equiv -h (\mathrm{mod}\, p)$

B) $p = (k-1)!h + 1$

a) k este număr par $\Rightarrow$ $(p-k)!(k-1)! \equiv 1-p(\bmod p)$ și, cum $(k-1)! | (1-p)$ și are loc relația (1), prin împărțire cu $(k-1)!$ avem: $(p-k)! \equiv -h(\bmod p)$.

b) k este număr impar $\Rightarrow$ $(p-k)!(k-1)! \equiv -1+p(\bmod p)$ și, cum $(k-1)! | (-1+p)$ și are loc relația (1), prin împărțire cu $(k-1)!$ avem $(p-k)! \equiv h(\bmod p)$.

Concentrând toate aceste cazuri, obținem: dacă p este prim, $p=(k-1)!h \pm 1$, cu $k>2$ și $h \in \mathbb{N}^*$, atunci

$$(p-k)! \equiv (-1)^{h+\left[\frac{p}{h}\right]+1} \cdot h(\bmod p).$$

Suficiența: Îmulțind congruența inițială cu $(k-1)!$ rezultă

$$(p-k)!(k-1)! \equiv (k-1)!h \cdot (-1)^{\left[\frac{p}{h}\right]+1} \cdot (-1)^k (\bmod p).$$

Analizând separat fiecare din cazurile:A) $p=(k-1)!h-1$ și B) $p=(k-1)!h+1$, se obține pentru amândouă, congruența:

$$(p-k)!(k-1)! \equiv (-1)^k (\bmod p)$$

care este echivalentă (am arătat la începutul acestei demonstrații) cu $(p-1)! \equiv -1(\bmod p)$ și rezultă că p este prim.

Bibliografie:

[1] Constantin P.Popovici -"Teoria numerelor" Editura didactică și pedagogică, București, 1973.

[Publicat în "Gazeta Matematică", Anul XXXVI, București, Nr.2, Februarie 1981, pg.49-52.]

INTEGER ALGORITHMS TO SOLVE LINEAR EQUATIONS AND SYSTEMS

Editions Scientifiques, 1984
Casablanca

FOREWORD

The present work includes some of the author's original researches on the integer solutions of equations and linear systems:

1. The notion of "general integer solution" of a linear equation with two unknowns is extendend to linear equations with n unknowns and then, to linear systems.
2. The proprieties of the general integer solution are determined (both of a linear equation and system).
3. Seven original integer algorithms (two for linear equations and five for linear systems) are presetend. The algorithms are carefully demonstrated and an example for each of them is given. These algorithms can be easily introduced into a computer.

INTEGER SOLUTIONS OF LINEAR EQUATIONS

Definitions and properties of the integer solutions of linear equations.

Consider the following linear equation:

(1) $\sum_{i=1}^{n} a_i x_i = b$, with all $a_i \neq 0$ and b in $\mathbf{Z}$

Again, let $h \in \mathbf{N}$, end $f_i : \mathbf{Z}^h \to \mathbf{Z}$, $i = \overline{1,n}$.

Definition 1

$x_i = x_i^o$, $i = \overline{1,n}$ is the particular integer solution of equation (1), if all $x_i^o \in \mathbf{Z}$ and $\sum_{i=1}^{n} a_i x_i^o = b$.

Definition 2

$x_i = f_i(k_1,\ldots,k_h)$, $i = \overline{1,n}$ is the general integer solution of equation (1) if:

(a) $\sum_{i=1}^{n} a_i f_i(k_1,\ldots,k_h) = b \ \forall (k_1,\ldots,k_h) \in \mathbf{Z}^h$,

(b) Irrespective of $f_i(x_1^o,\ldots,x_n^o)$ there is a particular integer solution for (1) $(k_1^o,\ldots,k_h^o) \in \mathbf{Z}^h$ so that $x_i^o = f_i(k_1^o,\ldots,k_h^o)$ for all $i = \overline{1,n}$.

We will further see that the general integer solution can be expressed by linear functions.

We consider for $1 \le i \le n$ the functions $f_i = \sum_{j=1}^{h} c_{ij} k_j + d_i$ with all c_{ij}, $d_i \in \mathbf{Z}$.

$\overline{1,n}$ means: form 1 to n

Definition 3

$A = (c_{ij})_{i,j}$ the matrix associated with the general solution of equation (1).

Definition 4

The integers $k_1,\ldots,k_s$, $1 \le s \le h$ are independent if all the corresponding column vectors of matrix A are linearly independent.

Definition 5

An integer solution is s - times undetermined if the maximal number of independent parameters is s.

Theorem 1. The general integer solution of equation (1) is undetermined $(n-1)$ - times.

Proof

We suppose that the particular integer solution is of the form:

(2) $x_i = \sum_{e=1}^{r} i_{ie}P_e + v_i$, $i = \overline{1,n}$, with all u_{ie}, $v_i \in \mathbf{Z}$,

P_e = are parameters of $\mathbf{Z}$, while a $a \le r < n-1$.

Let $(x_1^o,\ldots,x_n^o)$ be a general integer solution of equation

(1) (we are not interesed in the case when the equation does not have an integer solution). he solution

$$\begin{cases} x_j = a_n k_j + x_j^o, & j = \overline{1,n-1} \\ x_n = -(\sum_{j=1}^{n-1} a_j k_j - x_n^o) \end{cases}$$

is undetermined $(n-1)$ - times (it can be easily checked that the order of the associated matrix is $n-1$). Hence, there are n-1

undetermined solutions. Let, in the general case, a solution be undetermined $n-1$ times:

$$x_i = \sum_{j=1}^{n-1} c_{ij}k_j + d_i \ , \ i = \overline{1,n} \ \text{ with all } c_{ij}, d_i \in \mathbf{Z}$$

Consider the case when $b = 0$.

Then $\sum_{i=1}^{n} a_i x_i = 0$. It follows $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij}k_j + d_i \right) =$

$$= \sum_{i=1}^{n} a_i \sum_{j=1}^{n-1} c_{ij}k_j + \sum_{i=1}^{n} a_i d_i = 0.$$

For $k_j = 0, \ j = \overline{1,n-1}$ it follows that $\sum_{i=1}^{n} a_i d_i = 0$.

For $k_{j_0} = 1$ and $k_j = 0, \ j \neq j_o$, it follows that $\sum_{i=1}^{n} a_i c_{ij_0} = 0$.

Let the homogenous linear system of n equations with n unknowns be:

$$\begin{cases} \sum_{i=1}^{n} x_i c_{ij} = 0, & j = \overline{1,n-1} \\ \sum_{i=1}^{n} x_i d_i = 0 \end{cases}$$

which, obviously has solution $x_i = a_i, \ i = \overline{1,n}$ different from the trivial one. Hence the determinant of the system is zero, i.e., the vectors $c_j = (c_{1j},\dots,c_{nj})^t, \ j = \overline{1,n-1}, \ D = (d_1,\dots,d_n)^t$, are linearly dependent.

But the solution being n-1 times undetermined it shows that $c_j, \ j = \overline{1,n-1}$ are linearly independent. Then $(c_1,\dots,c_{n-1})$ determines a free submodule $\mathbf{Z}$ of the order $n-1$ in $\mathbf{Z}_n$ of solutions for the given equation.

Let us see what can be obtained from (2). We have:

$$0=\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i\left(\sum_{e=1}^{r} u_{ie}P_e + v_i\right)$$ As above, we obtain:

$\sum_{i=1}^{n} a_i v_i = 0$ and $\sum_{e=1}^{r} a_i u_{ie_o} = 0$ similarly, the vectors $U_h = (u_{1h},\dots,u_{nh})$ are linearly independent, $h = \overline{1,r}$, U_h, $h = \overline{1,r}$ are $V = (v_z,\dots,v_n)$ particular integer solutions of the homogenous linear equation.

Subcase (a1)

U, $h = \overline{1,r}$ are linearly dependent. This gives $\{U_1,\dots,U_r\}=$ the free submodule of order r in Z^n of solutions of the equation. Hence, there are solutions from $\{V_1,\dots,V_{n-1}\}$ which are not from $\{U_1,\dots,U_r\}$; this contradicts the fact that (2) is the general integer solution.

Subcase (a2)

U_h, $h = \overline{1,r}$, V are linearly independent. Then, $\{U_1,\dots,U_r\}$ + V is a linear variety of the dimension $<n-1$ = =dim $\{V_1,\dots,V_{n-1}\}$ and the conclusion can be similarly drawn.

Consider the case when $b \neq 0$.

So, $\sum_{i=1}^{n} a_i x_i = b$. Then $\sum_{i=1}^{n} a_i\left(\sum_{j=1}^{n-1} c_{ij}k_j + d_i\right) = \sum_{j=1}^{n-1}\left(\sum_{i=1}^{n} a_i c_{ij}\right)k_j +$

$+ \sum_{i=1}^{n} a_i d_i = b$, $\forall (k_1,\dots,k_{n-1}) \in \mathbf{Z}^{n-1}$. As in the previous case, we get $\sum_{i=1}^{n} a_i d_i = b$ and $\sum_{i=1}^{n} a_i c_{ij} = 0$, $\forall j = \overline{1,n-1}$. The vectors $c_j = (c_{ij},\dots,c_{nj})^t$, $j = \overline{1,n-1}$, are lnearly independent because the solution is undetermined $n-1$ times.

Conversely, if $c_1,\dots,c_{n-1}$, D (where $D = (d_1,\dots,d_n)^t$ were

linearly dependent, it would mean that $D = \sum_{j=1}^{n-1} s_j c_j$ with all s_j scalar; it would also men that $b = \sum_{i=1}^{n} a_i d_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} s_j c_{ij} \right) =$

$$= \sum_{j=1}^{n-1} s_j \left(\sum_{i=1}^{n} a_i c_{ij} \right) = 0.$$

This is impossible.

(3) Then $\{c_1, \ldots, c_{n-1}\} + D$ is a linear variety.

Let us see what we can obtain from (2). We have:

$$b = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i \left(\sum_{e=1}^{r} u_{ie} P_e + v_i \right) = \sum_{e=1}^{r} \left(\sum_{i=1}^{n} a_i u_{ie} \right) P_e + \sum_{i=1}^{n} a_i v_i$$

and, similarly: $\sum_{i=1}^{n} a_i v_i = b$ and $\sum_{i=1}^{n} a_i u_{ie} = 0$, $\forall e = \overline{1, r}$, respectively. The vectors $U_e = (u_{1e}, \ldots, u_{ne})^t$, $e = \overline{1, r}$ are linearly independent because the solution is undetermined r-times.

A procedure like that applied in (3) shows that $U_1, \ldots, U_r$, V are linearly independent, where $V = (v_1, \ldots, v_n)^t$. Then $\{U_1, \ldots, U_r\} + V =$ a linear variety = free submodule of order $r < n-1$. That is, we can find vectors from $c_1, \ldots, c_{n-1} + D$ which are not from $\{U_1, \ldots, U_r\} + V$, contradicting the "general" characteristic of the integer number solution. Hence, the general integer solution is undetermined $n-1$ times.

Theorem 2. The general integer solution of the homogenous linear equation $\sum_{i=1}^{n} a_i x_i = 0$ (all $a_i \in \mathbf{Z} \setminus \{0\}$) can be written under the from:

(4) $x_i = \sum_{j=1}^{n-1} c_{ij} k_j$, $i = \overline{1, n}$ (with $d_1 = \ldots = d_n = 0$).

Definition 6. This is called the standard form of the general integer solution of a homogenous linear equation.

Proof:

We consider the general integer solution under the form: $x_i = \sum_{j=1}^{n-1} c_{ij}P_j + d_i$, $i = \overline{1,n}$ with not all $d_i = 0$. We show that it can be written under the form (4). The homogenous equation has the trivial solution $x_i = 0$, $i = \overline{1,n}$. There is $(p_1^o, \ldots, p_{n-1}^o) \in \mathbf{Z}^{n-1}$ so that $\sum_{j=1}^{n-1} c_{ij}p_j^o + d_i = 0$, $\forall i = \overline{1,n}$. Substituting: $P_j = k_j + p_j$, $j = \overline{1,n-1}$ in the form from the beginning of the demonstration we will obtain form (4). We have to mention that the substitution does not diminish the degree of generality as $P_j \in \mathbf{Z} \Leftrightarrow k_j \in \mathbf{Z}$ because $j = \overline{1,n-1}$.

Theorem 3. The general integer solution of a nonhomogeneous linear equation is equal to the general integer solution of its associated homogenous linear equation + any particular integer solution of the nonhomogeneous linear equation.

Proof:

Let $x_i = \sum_{j=1}^{n-1} c_{ij}k_j$, $i = \overline{1,n}$, be the general integer solution of the associated homogenous linear equation and, again, let $x_i = v_i$, $i = \overline{1,n}$, be a particular integer solution of the nonhomogeneous linear equation. Then, $x_i = \sum_{j=1}^{n-1} c_{ij}k_j + v_i$, $i = \overline{1,n}$, is the general integer solution of the nonhomogeneous linear equation.

Actually, $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij} k_j + v_i \right) = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n-1} c_{ij} k_j \right) +$ $+ \sum_{i=1}^{n} a_i v_i = b$; if $x_i = x_i^o$, $i = \overline{1,n}$, is a particular integer solution of the nonhomogeneous linear eguation, then $x_i = x_i - v_i$, $i = \overline{1,n}$, is a particular integer solution of the homogenous linear equation: hence, there is $(k_1^o, \dots, k_{n-1}^o) \in \mathbf{Z}^{n-1}$ so that $\sum_{j=1}^{n-1} c_{ij} k_j^o = x_i^o - v_i$, $\forall i = \overline{1,n}$, i.e., $\sum_{j=1}^{n-1} c_{ij} k_j^o + v_i = x_i^o$, $\forall i = \overline{1,n}$, which was to be proven.

Theorem 4. If $x_i = \sum_{j=1}^{n-1} c_{ij} k_j$, $i = \overline{1,n}$ is the general integer solution of a homogenous linear equation $(c_{ij}, \dots, c_{nj}) \sim 1$, $\forall j = \overline{1, n-1}$.

The demonstration is made by reductio ad absurdum. If $\exists j_o$, $1 \le j_o \le n-1$, so that $(c_{ij_0}, \dots, c_{nj_0}) \sim d_{j_0} \neq \pm 1$, then $c_{ij_0} = c'_{ij_0} d_{ij_0}$ with $(c'_{ij_0}, \dots, c'_{nj_0}) \sim 1$, $\forall i = \overline{1,n}$.

But $x_i = c'_{ij_0}$, $i = \overline{1,n}$, represents a particular integer solution as $\sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} a_i c'_{ij_0} = 1 / d_{j_0} \cdot \sum_{i=1}^{n} a_i c_{ij_0} = 0$ (because $x_i = c_{ij_0}$, $i = \overline{1,n}$, is a particular integer solution from the general integer solution by introducing $k_{j_0} = 1$ and $k_j = 0$, $j \neq j_o$. But the particular integer solution $x_i = c'_{ij_0}$, $i = \overline{1,n}$, cannot be obtained by introducing integer number parameters (as it should) from the general integer solution, as from the linear system of n equations and $n-1$ unknowns, which is compatible. We obtain:

$$x_i = \sum_{\substack{j=1\\ j\neq j_0}}^{n} c_{ij}k_j + c'_{ij_0} d_{j_0} k_{j_0} = c'_{ij_0},\ i = \overline{1,n}.$$

Leaving aside the last equation--which is a linear combination of the other $n-1$ equations--a Kramerian systemis obtained. It follows:

$$k_{j_0} = \frac{\begin{vmatrix} c_{11} \cdots c'_{ij_0} \cdots c_{1,n-1} \\ \vdots \\ c_{n-1,1} \cdots c_{n-1j_0} \cdots c_{n-1,n-1} \end{vmatrix}}{\begin{vmatrix} c_{11} \cdots c'_{ij_0} d_{j_0} \cdots c_{1,n-1} \\ \vdots \\ c_{n-1,1} \cdots c'_{n-1j_0} d_{j_0} \cdots c_{n-1,n-1} \end{vmatrix}} = \frac{1}{d_{j_0}} \notin \mathbf{Z}$$

The assumption is false [End of the demonstration.]

Theorem 5. Considering the equation (1) with $(a_1,\ldots,a_n)\sim 1$, $b = 0$ and the general integer solution $x_i = \sum_{j=1}^{n-1} c_{ij}k_j$, $i = \overline{1,n}$, then $(a_1,\ldots,a_{i-1},a_{i+1},\ldots,a_n)$ ~ $(c_{i1},\ldots,c_{in-1})$, $\forall i = \overline{1,n}$. The demonstration is made by double divisibility. Let i_o, $1 \leq i_o \leq n$ be arbitrary but fixed. $x_{i_0} = \sum_{j=1}^{n-1} c_{i_0 j}k_j$. Consider the equation $\sum_{i\neq i_0} a_i x_i = -a_{i_0} x_{i_0}$. We have shown that $x_i = c_{ij}$, $i = \overline{1,n}$ is a particular integer solution irrespective of j, $a \leq j \leq n-1$. The equation $\sum_{i\neq i_0} a_i x_i = -a_{i_0} c_{i_0 j}$ obviously, has the integer solution $x_i = c_{ij}$, $i \neq i_0$. Then $(a_1,\ldots,a_{i_0-1},a_{i_0+1},\ldots,a_n)$ divides $-a_{i_0}c_{i_0 j}$ as we have assumed that it follows that $(a_1,\ldots,a_n)\sim 1$, it follows that

$(a_1,\dots,a_{i_0-1},a_{i_0+1},\dots,a_n)|c_{i_0j}$ irrespective of j.

Hence $(a_1,\dots,a_{i_0-1},a_{i_0+1},\dots,a_n)|(c_{i_01},\dots,c_{i_0n-1})$, $\forall i=\overline{1,n}$, and the divisibility in one sense was proven.

Inverse Divisibility:

Let us suppose the contrary and say that $\exists i_1 \in \overline{1,n}$ for which $(a_1,\dots,a_{i_1-1},a_{i_1+1},\dots,a_n) \sim d_{i_11} \neq d_{i_12} \sim (c_{i_11},\dots,c_{i_1n-1})$; we have considered d_{i_11} and d_{i_12} without restricting the generality.

$d_{i_11}|d_{i_12}$ according to yhe first part of the demonstration. Hence, $\exists d \in \mathbf{Z}$ so that $d_{i_12} = d\cdot d_{i_11}$, $|d| \neq 1$.

$$x_{i_1} = \sum_{j=1}^{n-1} c_{i_1j}k_j = d\cdot d_{i_11}\sum_{j=1}^{n-1} c'_{i_1j}k_j;\ \sum_{i=1}^{n} a_ix_i = 0 \Rightarrow \sum_{i\neq i_1}^{n} a_ix_i =$$

$$= -a_{i_1}x_{i_1}\ \sum_{i\neq i_1} a_ix_i = -a_{i_1}d\cdot d_{i_11}\sum_{j=1}^{n-1} c'_{i_1j}k_j,\ \text{where } (c_{i_11},\dots,c_{i_1n-1})\sim 1.$$

The nonhomogeneous linear equation $\sum_{i\neq i_1} a_ix_i = -a_{i_1}d_{i_1}$ has theinteger solution because $a_{i_1}d_{i_1}$ is divisible by $(a_1,\dots,a_{i_1-1},a_{i_1+1},\dots,a_n)$. Let $x_i = x_i^o$, $i\neq i_1$, be its particular integer solution. It follows that the equation $\sum_{i=1}^{n} a_ix_i = 0$ the particular solution $x_i = x_i^o$, $i\neq i_1$, $x_{i_1} = d_{i_1}$, which is written as (5). We show that (5) cannot be obtained from the general solution by integer number parameters:

$$\begin{cases} \sum_{j=1}^{n-1} c_{ij}k_j = x_i^o, i\neq i_1 \\ d\cdot d_{i_11}\sum_{j=1}^{n-1} c_{ij}k_j = d_{i_11} \end{cases} \tag{6}$$

But equation (6) does not have an integer solution because $d \cdot d_{i_1 1} | d_{i_1 1}$ thus, contradicting, the "general" characteristic of the integer solution.

As a conclusion we can write:

Theorem 6. Let the homogenous linear equation be: $\sum_{i=1}^{n} a_i x_i = 0$, with all $a_i \in \mathbf{Z} \setminus \{0\}$ and $(a_1, \ldots, a_n) \sim 1$.

Let $x_i = \sum_{j=1}^{h} c_{ij} k_j$, $i = \overline{1,n}$ with all $c_{ij} \in \mathbf{Z}$, all k_j integer parameters and $h \in \mathrm{N}$ be a general integer solution of the equation. Then,

1) the solution is undetermined $n-1$ times

2) $\forall j = \overline{1, n-1}$ we have $(c_{1j}, \ldots, c_{nj}) \sim 1$;

3) $\forall i = \overline{1,n}$ we have $(c_{i1}, \ldots, c_{in-1}) \sim (a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n)$

The proof results from Theorems 1,4 and 5.

Note 1. The only equation of the form (1) is undetermined n times is the trivial equation $0 \cdot x_1 + \ldots + 0 \cdot x_n = 0$.

Note 2. The converse of theorem 6 is not true.

Counterexemple:

$$\begin{cases} x_1 = -k_1 + k_2 \\ x_2 = 5k_1 + 3k_2 \\ x_3 = 7k_1 - k_2; \qquad k_1, k_2 \in \mathbf{Z} \end{cases} \tag{7}$$

is not the general integer solution of the equation

$$-13x_1 + 3x_2 - 4x_3 = 0 \tag{8}$$

although the solution (7) verifies the points 1), 2) and 3) of theorem 6. (1, 7, 2) is the particular integer solution of (8) but cannot be obtained by introducing integer number parameters in (7) because from

$$\begin{cases} -k_1 + k_2 = 1 \\ 5k_1 + 3k_2 = 7 \\ 7k_1 - k_2 = 2 \end{cases}$$

it follows that $k = 1/2 \notin \mathbf{Z}$ and $k = 3/2 \notin \mathbf{Z}$ (unique roots).

Reference:

[1] Smarandache, Florentin--Whole number solution of liniear equations and systems--diploma paper, 1979, University of Craiova (under the supervision of Assoc. Prof. Dr. Alexandru Dincă).

AN INTEGER NUMBER ALGORITHM TO SOLVE LINEAR EQUATIONS

An algorithm is given ascertains whether a linear equation has integer number solutions or not; if it does, the general integer solution is determined.

Input

A linear equation $a_1x_1+\ldots+a_nx_n = b$, with a_i $b \in \mathbf{Z}$, x_i being integer number unknowns, $i = \overline{1,n}$, and not all $a_i = 0$.

Output

Decision on the integer solution of this equation; and if the equation has solutions in $\mathbf{Z}$, its general solution is obtained.

Method

Step 1. Calculate $d = (a_1, \ldots, a_n)$.

Step 2. If d / b then "the equation has integer solution"; go on to Step 3. If d / b then "the equation does not have integer solution"; stop.

Step 3. Consider $h := 1$. If $|d| \neq 1$, divide the equation by d; consider $a_i := a_i / d$, $i = \overline{1,n}$, $b := b / d$.

Step 4. Calculate $a = \min\limits_{a_s \neq 0} |a_s|$ and determine an i so that $a_i = a$.

Step 5. If $a \neq 1$, go to Step 7.

Step 6. If $a = 1$, then:

(A) $x_i = -(a_1x_1 + \ldots + a_{i-1}x_{i-1} + a_{i+1}x_{i+1} + \ldots + a_nx_n - b) \cdot a_i$

(B) Substitute the value of x_i the values of the other determined unknowns.

(C) Substitute integer number parameters for all the variables of the unknown values in the right term: $k_1, k_2, \ldots, k_{n-2}$, and k_{n-1}, respectively.

(D) Write down the general solution thus determined; stop.

Step 7. Write down all a_j, $j \neq i$ and under the form:

$$a_j = a_i q_j + r_j$$

$$b = a_i q + r \text{ where } q_j = \left[\frac{a_j}{a_i}\right],\ q = \left[\frac{b}{a_i}\right].$$

Step 8. Write $x_i = -q_1 x_1 - \ldots - q_{i-1} x_{i-1} - q_{i+1} x_{i+1} - \ldots - q_n x_n + q - t_h$. Substitute the value of x_i in the values of the other determined unknowns.

Step 9. Consider

$$\begin{cases} a_1 := r_1 \\ \vdots \\ a_i - 1 := r_{i-1} \\ a_{i+1} := r_{i+1} \\ \vdots \\ a_n := r_n \end{cases} \quad \text{and} \quad \begin{cases} a_i := -a_i \\ b := r \\ x_i := t_h \\ h := h+1 \end{cases}$$

and go back to Step 4.

Lemma 1. The previous algorithm is finite.

Proof:

Let the initial linear equation be $a_1 x_1 + \ldots + a_n x_n = b$, with not all $a_i = 0$; check for $\min\limits_{a_s \neq 0} |a_s| = a_1 \neq 1$ (if not, it is renumbered). Following the algorithm, once we pass from this initial equation to a new equation: $a_1' t_1 + a_2' x_2 + \ldots + a_n' x_n = b'$, with $|a_1'| < |a_i|$ for $i = \overline{2,n}$, $|b'| < |b|$ and $a_1' = -a_1$.

It follows that $\min_{a'_s \neq 0} |a'_s| < \min_{a_s \neq 1} |a_s|$. We continue similarly and after a finite numer of steps we get, at Step 4, $a := 1$ (as, every, at this the actual a is always smaller than the previous a, according to the Former note) and in this case algorithm terminates.

Lemma 2. Let the linear equation be:

(25) $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, with $\min_{a_s \neq 0} |a_s| = a_1$ and the equation: (26) $-a_1t_1 + r_2x_2 + \ldots + r_nx_n = r$, with $t_1 = -x_1 - q_2x_2 - \ldots - q_nx_n + q$, where $r_i = a_i - a_iq_i$, $i = \overline{2,n}$, $r = b - a_1q$ while $q_i = \left[\frac{a_i}{a}\right]$, $r = \left[\frac{b}{a_1}\right]$. Then $x_1 = x_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$ is a particular solution of equation (25) if and only if $t_1 = t_1^o = -x_1 - q_2x_2^o - \ldots - q_nx_n^o + q$, $x_2, \ldots, x_n = x_n^o$, is a particular solution of equation (26).

Proof:

$x_1 = x_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$, is a particular solution of equation (25) $\Leftrightarrow$ $a_1x_1^o + a_2x_2^o + \ldots + a_nx_n^o = b$ $\Leftrightarrow$ $a_1x_1^o + (r_2 + a_1q_2)x_2^o + \ldots + (r_n + a_1q_n)x_n^o = a_1q + r$ $\Leftrightarrow$ $r_2x_2^o + \ldots + r_nx_n^o - a_1(-x_1^o - q_2x_2^o - \ldots - q_nx_n^o + q) = r$ $\Leftrightarrow$ $-a_1t_1^o + r_2x_2^o + \ldots + r_nx_n^o = r$ $\Leftrightarrow$ $t_1 = t_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$ is a particular solution of equation (26).

Lemma 3. $x_i = c_{i1}k_1 + \ldots + c_{in-1}k_{n-1} + d_i$, $i = \overline{1,n}$, is the general solution of equation (25) if and only if:

(28) $$t_1 = -(c_{11} + q_2c_{21} + \ldots + q_nc_{n1})k_1 - \ldots - (c_{1n-1} + q_2c_{2n-1} + \ldots + q_nc_{nn-1})K_n - (d_1 + q_2d_2 + \ldots + q_nd_n) + q,$$
$$x_j = c_{cj1}k_1 + \ldots + c_{jn-1}k_{n-1} + d_j,\ j = \overline{2,n}$$

is a general solution for equation (26).

Proof:

$t_1 = t_1^o = -x_1^o - q_2x_2^o - \ldots - q_nx_n^o + q$, $x_2 = x_2^o, \ldots, x_n = x_n^o$, is a particular solution of the equation (25) $\Leftrightarrow$ $x_1 = x_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$ is a particular solution of equation (26) $\Leftrightarrow$ $\exists k_1 = k_1^o \in \mathbf{Z}, \ldots, k_n = k_n^o \in \mathbf{Z}$ so that $x_i = c_{i1}k_1^o + \ldots + c_{in-1}k_{n-1}^o + d_i = x_i^o$, $i = \overline{1,n}$ $\Leftrightarrow$ $\exists k_1 = k_1^o \in \mathbf{Z}, \ldots, k_n = k_n^o \in \mathbf{Z}$, so that $x_i = c_{i1}k_1^o + \ldots + c_{in-1}k_{n-1}^o + d_i = x_i^o$, $i = \overline{2,n}$, and $t_1 = -(c_{11} + q_2c_{21} + \ldots + q_nc_{n1})k_1^o - \ldots - (c_{1n-1} + q_2c_{2n-1} + \ldots + q_nc_{nn-1})k_{n-1}^o - (d_1 + q_2d_2 + \ldots + q_nd_n) + q = -x_1^o - q_2x_2^o - \ldots - q_nx_n^o + q = t_1^o$.

Lemma 4. The linear equation

(29) $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$ with $|a_1| = 1$ has the general solution:

$$(30) \qquad \begin{cases} x_1 = -(a_2k_2 + \ldots + a_nk_n - b)a_1 \\ x_i = k_i \in \mathbf{Z} \\ i = \overline{2,n} \end{cases}$$

Proof:

Let $x_1 = x_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$, be a particular solution of the equation (29). $\exists k_2 = x_2^o$, $k_n = x_n^o$, so that $x_1 = -(a_2x_2^o + \ldots + a_nx_n^o - b)a_1 = x_1^o$, $x_2 = x_2^o, \ldots, x_n = x_n^o$.

Lemma 5. Let the linear equation be $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, with $\min_{a_s \neq 0}|a_s| = a_1$ and $a_i = a_1q_i$, $i = \overline{2,n}$.

Then, the general solution of the equation is:

$$\begin{cases} x_1 = -(q_2k_2 + \ldots + q_nk_n - q) \\ x_i = k_i \in \mathbf{Z} \\ i = \overline{2,n} \end{cases}$$

Proof:

Dividing the equation by a_1 the conditions of Lemma 4 are met.

Theorem of Correctness. The preceding algorithm correctly calculates the general solution of the linear equation $a_1x_1 + \ldots + a_nx_n = b$, with not all $a_i = 0$.

Proof:

The algorithm is finite according to Lemma 1. The correctness of steps 1,2, and 3 is obvious. At step 4 there is always $\min\limits_{a_s \neq 0} |a_s|$ as not all $a_i = 0$. The correctness of substep 6 A) results from Lemma 4 and 5, respectively. This algorithm represents a method of obtaining the general solution of the initial equation by means of the general solutions of the linear equation obtained after the algorithm was followed several times (according to Lemmas 2 and 3); from Lemma 3, it follows that to obtain the general solution of an initial linear equation is equivalent to calculate the general solution of an equation at step 6 A), equation whose general solution is given in algorithm (according to Lemmas 4 and 5). The theorem of correctness has been fully proven.

Note. At step 4 of the algorithm we consider $a := \min\limits_{a_s \neq 0} |a_s|$ so that the number of iterations is as small as possibile. The algorithm works if we consider $a := |a_i| \neq \max\limits_{s = \overline{1,n}} |a_s|$ but it takes longer. The algorithm can be introduced into a computer program.

Application

Calculate the integer solution of the equation:

$$6x_1 - 12x_2 - 8x_3 + 22x_4 = 14.$$

Solution

The former algorhytm is applied.

1. $(6, -12, -8, 22) = 2$

2. $2 \mid 14$ so that the solution of the equation is in $\mathbf{Z}$.

3. $h := 1$; $\mid 2 \mid \neq 1$; dividing the equation by 2 we get:

$$3x_1 = 6x_2 - 4x_3 + 11x_4 = 7$$

4. $a := \min\{|3|, |-6|, |-4|, |11|\} = 3,\ i = 1$

5. $a \neq 1$

7. $-6 = 3.(-2) + 0$

$-4 = 3.(-2) + 2$

$11 = 3.3 + 2$

$7 = 3.2 + 1$

8. $x_1 = 2x_2 + 2x_3 - 3x_4 + 2 - t_1$

9. $a_2 := 0 \qquad a_1 := -3$

$a_3 := 2 \qquad b := 1$

$a_4 := 2 \qquad x_1 := t_1$

$h := 2$

4. We have a new equation:

$$-3t_1 + 0 \cdot x_2 + 2x_3 + 2x_4 = 1$$

$a := \min\{|-3|, |2|, |2|\}$ and

$i = 3$

5. $a \neq 1$

7. $-3 = 2 \cdot (-2) + 1$

$0 = 2 \cdot 0 + 0$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 0$

8. $x_3 = 2t_1 + 0 \cdot x_2 - x_4 + 0 - t_2$. Substituting the value of x_3 in the value determined for x_1 we get:

$$x_1 = 2x_2 - 5x_4 + 3t_1 - 2t_2 + 2$$

9. $a_1 := 1 \qquad a_3 := -2$

$a_2 := 0 \qquad b := 1$

$a_4 := 0 \qquad x_3 := t_2$

$h := 3$

4. We have obtained the equation:

$1 \cdot t_2 + 0x_2 - 2t_2 + 0 \cdot x_4 = 1,$

$a = 1$, and

$i = 1$

6. (A) $t_1 = -(0 \cdot x_2 - 2t_2 + 0 \cdot x_4 - 1) \cdot 1 = 2t_2 + 1$

(B) Substituting the value of t_1 inthe values of x_1 and x_3 previously determined, we get:

$x_1 = 2x_2 - 5x_4 + 4t_2 + 5$ and

$x_3 = -x_4 + 3t_2 + 2$

(C) $x_2 := k_1$, $x_4 := k_2$, $t_2 = k_3$, $k_1, k_2, k_3 \in \mathbf{Z}$

(D) The general solution of the initial equation is:

$x_1 = 2k_1 - 5k_2 + 4k_3 + 5$

$x_2 = k_1$

$x_3 = -k_2 + 3k_3 + 2$

$x_4 = k_2$

k_1, k_2, k_3 are parameters $\in \mathbf{Z}$

Reference:

[1] Smarandache, Florentin, Whole number solution of equations and systems of equations--diploma paper, University of Craiova, 1979.

ANOTHER INTEGER NUMBER ALGORITHM TO SOLVE LINEAR EQUATIONS (USING CONGRUENCY)

In this section a new integer number algorithm for linear equations is presented. This is more "rapid" than W.Sierpinski's presented in [1] in the sense that it reaches the general solution after a smaller number of iterations. Its correctness will be thorovghly demonstrated.

INTEGER NUMBER ALGORITHM TO SOLVE LINEAR EQUATIONS

Let us consider the equation (1); (the case $a_i, b \in \mathbf{Q}$, $i = \overline{1,n}$ is reduced to the case (1) by reducing to the same denominator and eliminating the denominators). Let $d = (a_1, \dots, a_n)$ If $d | b$ then the equation does not have integer solutions, while if $d | b$ the equation has integer solutions (according to a well-known theorem from the theory of numers).

If the equation has solutions and $d \neq$ we divide the equation by d. Then $d = 1$ (we do not make any restriction if we consider the maximal co-divisor positive).

(a) Also, if all a_i the equation is trivial; it has the general integer solution $x_i = k_i \in \mathbf{Z}$, $i = \overline{1,n}$, when $b = 0$ (the only case when the general integer solution is n - times undetermined) and does not have solution when $b \neq 0$.

(b) If $\exists i$, $1 \le i \le n$ so that $a_i = \pm 1$ then the general integer solution is:

$$x_i = -a_i\Big(\sum_{\substack{j=1 \\ j \neq i}}^{n} a_j k_j - b\Big) \text{ and } x_s = k_s \in \mathbf{Z},\ s \in \{1, \dots, n\} \setminus \{i\}$$

The proof of this assertion was given in [4]. All these cases are trivial, so we will leave them aside. The following algorithm can be written:

Input

A linear equation: (2)

$\sum_{i=1}^{n} a_i x_i = b$, $a_i, b \in \mathbf{Z}$, $a_i \neq \pm 1$, $i = \overline{1,n}$, with not all $a_i = 0$ and $(a_1,\ldots,a_n) = 1$.

Output

The general solution of the equation

Method

1. $h := 1$, $p := 1$
2. Calculate $\min\limits_{1 \le i, j \le n} \left\{ |r|, r \equiv a_i (\mathrm{mod}\, a_j), r \neq 0, |r| < |a_j| \right\}$ and determine r and the pair (i, j) for which this minimum can be obtained (when there are more possibilities we have to choose one of them).
3. If $|r| \neq$ go on to step 4.
   If $|r| = 1$, then

$$\begin{cases} x_i := r(-a_j t_h - \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s + b) \\ x_j := r(a_i t_h + \dfrac{a_i - r}{a_j} \cdot \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s + \dfrac{r - a_i}{a_j} b) \end{cases}$$

   (A) Substitute the values thus determinied of these unknowns in all the statements (p), $p = 1,2,\ldots$ (if possible).

   (B) From the last relation (p) obtained in the algorhythm substitute in all relations:

$(\bar{p}-1), (\bar{p}-2), \ldots, (1)$

(C) Every statement, starting in order from $(\bar{p}-1)$ should be applied the same procedure as in (B): then $(\bar{p}-2), \ldots, (3)$ respectively.

(D) Write the values of the unknowns x_i, $i = \overline{1,n}$, from the initial equation (writing the corresponding integer number parameters from the right term of these unknowns with $k_1, \ldots, k_{n-1}$), STOP.

4. Write the statement (p):

$$x_j = t_h - \frac{a_i - r}{a_j} x_i$$

5. Assign $x_j := t_h$ $\qquad h := h + 1$

$a_i := r$ $\qquad p := p + 1$

The other coefficients and variables remain unchanged go back to step 2.

The Correctness of the Algorithm

Let us consider linear equation (2). Under these conditions, the following propecties exist:

Lemma 1. The set $M = \{|r|, r \equiv a_i (\operatorname{mod} a_j), 0 < |r| < |a_j|\}$ has a minimum.

Proof:

Obviously $M \subset N^*$ and M is finite because the equation has a finite number of coefficients: n, and considering all the possible combinations of these, by twos, there is the maximum AR_n^2 (arranged with repetition) $= n^2$ elements.

Let us show, by reductio ad absurdum, that $M \neq \varnothing$.

$M = \varnothing \quad \Leftrightarrow \quad a_i \equiv 0 (\operatorname{mod} a_j) \forall i, \quad j \in \overline{1,n}$. Hence $a_j \equiv 0 (\operatorname{mod} a_i) \forall i$, $j \in \overline{1,n}$. Or this is possible only when

$|a_i| = |a_j|$, $\forall i, j \in \overline{1,n}$, [illegible] is [illegible]valent to $(a_1, \ldots, a_n) = a_i$, $\forall i \in \overline{1,n}$. But $(a_1, \ldots, a_n) = 1$ [illegible] a restriction from the assumption. It follows that $|a_i| = \overline{1,n}$, $\forall i \in \overline{1,n}$ a fact which contradicts the other restrictions of the assumption.

$M \neq 0$ and finite, it follows that M has a minimum.

Lemma 2. If $|r| = \min\limits_{1 \le i,j \le n} M$, then $|r| < |a_i|$, $\forall i \in \overline{1,n}$.

Proof:

We assume, conversely, that $\exists i_o$, $1 \le i_o \le n$ so that $|r| \ge |a_{i_0}|$. Then $|r| \ge \min\limits_{1 \le j \le n} \{|a_j|\} = |a_{j_0}| \neq 1$, $1 \le j_0 \le n$. Let a_{p_0}, $1 \le p_0 \le n$, so that $|a_{p_0}| > |a_{j_0}|$ and a_{p_0} is not divided by a_j^o. There is a coefficient in the equation, $|a_{j_0}|$ whick is the minimum and the coefficients are inot equa among themselves (conversely, it would mean that $(a_1, \ldots, a_n) = a_1 = \pm 1$ which is aqainst the hypothesis and, again, of the coefficients whose absolute valve is greater than $|a_{ij_0}|$ not all can be divided by a_{j_0} (conversely, it would similarly result in $(a_1, \ldots, a_n) = a_{j_0} \neq \pm 1$. We write $\left[a_{p_0} / a_{j_0}\right] = q_0 \in \mathbf{Z}$ (integer portion), and $r = a_{p_0} - q_o a_{j_0} \in \mathbf{Z}$. We have $a_{p_0} \equiv r_o (\operatorname{mod} a_{j_0})$ and $0 < |r_0| < |a_{j_0}| < |a_{i_0}| \le |r|$. Thus, we have found a r_0 which $|r_0| < |r|$ contradicts the definition of minimum given to $|r|$.

Thus, $|r| < |a_i|$, $\forall i \in \overline{1,n}$.

Lemma 3. If $|r| = \min M = 1$ for the pair of indices (i, j), then:

$$\begin{cases} x_i = r(-a_j t_h - \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s k_s + b) \\ x_j = r(a_i t_h + \dfrac{a_i - r}{a_j} \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s k_s + \dfrac{r - a_i}{a_j} b) \\ x_s = k_s \in \mathbf{Z}, s \in \{1,\ldots,n\} \setminus \{i,j\} \end{cases}$$

is the general integer solution of equation (2).

Proof:

Let $x_e = x_e^o$, $e = \overline{1,n}$, be a particular integer solution of equation (2). Then $\exists k_s = x_s^o \in \mathbf{Z}$, $s \in \{1,\ldots,n\} \setminus \{i,j\}$ and $t_h = x_j^o + \dfrac{a_i - r}{a_j} x_i^o \in \mathbf{Z}$ (because $a_i - r = Ma_j$) so that:

$$x_i = r - a_j(x_j^o + \frac{a_i - r}{a_j} x_i) - \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^o + b = x_i^o$$

$$x_j = r - a_j(x_j^o + \frac{a_i - r}{a_j} x_i^o) + \frac{a_i - r}{a_j} - \sum_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s x_s^o + \frac{r - a_i}{a_j} b = x_i^o$$

and $x_s = k_s = x_s^o$, $s \in \{1,\ldots,n\} \setminus \{i,j\}$.

Lemma 4. Let $|r| \neq$ and (i,j) be the pair of indices for which this minimum can be obtained. Again, let the system of linear equations be:

$$(3) \qquad \begin{cases} a_j t_h + r x_i + \sum\limits_{\substack{s=1 \\ s \notin \{i,j\}}}^{n} a_s k_s = b \\ t_h = x_j + \dfrac{a_i - r}{a_j} x_i \end{cases}$$

Then, $x_e = x_e^o$, $e = \overline{1,n}$ is a particular integer solution for (2) if and only if $x_e = x_e^o$, $e \in \{1,\dots,n\} \setminus \{j\}$ and $t_h = t_h^o = x_j^o + \dfrac{a_i - r}{a_j} x_i$ is the particular integer solution of (3).

Proof:

$x_e = {}^*x_e$, $e = \overline{1,n}$ is a particular integer solution for (2)

$$\Leftrightarrow \sum_{e=1}^{n} a_e x_e^o = b \Leftrightarrow \sum_{\substack{s=1 \\ s \neq \{i,j\}}}^{n} a_s x_s^o + a_j\left(x_j^o + \frac{a_i - r}{a_j} x_i^o\right) + r x_i^o = b$$

$$\Leftrightarrow a_j t_h^o + r x_i^o + \sum_{\substack{s=1 \\ s \neq \{i,j\}}}^{n} a_s x_s^o = b \text{ and } t_h^o = x_j^o + \frac{a_i - r}{a_j} x_i^o \in \mathbf{Z}$$

$$\Leftrightarrow x_e = x_e^o,\ e \in \{1,\dots,n\} \setminus \{j\}$$

and $t_h = t_h^o$ is a particular integer solution for (3).

Lemma 5. The former algorithm is finite.

Proof:

When $|r| = 1$ the algorithm stops at step 3. We will discuss the case when $|r| \neq 1$. According to the definition of r, $|r| \in \mathbf{N}^*$. We show that the row of $r - s$ successively obtained by following the algorithm several times is decreasing with cycle, and each cycle is not equal to the previous, to 1. Let r_1 be the first obtained by following the algorithn one time. $|r_1| \neq 1$ go on to steps 4 and, then 5. According to lemma 2 $|r_1| < |a_i|$, $\forall i = \overline{1,n}$. Now we shall follow the algorithm a second time, but this time for an equation in which r_1 (according to step 5) is substituted for a_i. Again, according to lemma 2, the new $|r|$ written $|r_2|$ will have the proprietty: $|r_2| < |r_1|$. We will get to

$|r| = 1$ because $|r| \geq 1$ and $|r| < \infty$, and if $|r| \neq 1$, following the algorithm once again we get $|r| < |r_1|$ a.s.o. Hence, the algorhytm has a finite number of repetitions.

Theorem of Correctness. The former algorithm calculates the general integer solution of thelinear equation correctly (2).

Proof:

According to lemma 5 the algorithm is finite. From lemma 1 it follows that the set M has a minimum, hence step 2 of the algorithm has meaning. When $|r| = 1$ it was shown in lemma 3 that step 3 of the algorithm calculates the general integer solution of the respective equation correctly the equation that appears at step 3). In lemma 4 it is shown that if $|r| \neq 1$ the substitutions steps 4 and 5 introducedin the initial equation, the general integer solution remains unchanged. That is, we pass from the initial equation to a linear system having the same general solution as the initial equation. The variable h is a counter of the newly introduced variables which are used to successively decompose the system in systems of two linear equations. The variable p is a counter of the substitutions of variables (the relations, at a given moment, between certain variables).

When the initial equation was decomposed to $|r| = 1$, we have to proceed in the reverse way: i.e., to compose itsgeneral integer solution. This reverse way is directed by the substeps 3(A), 3(B) and 3(C). The substep 3(D) has only an aesthetic role, i.e., to have the general solution under the from: $x_i = f_i(k_1,\ldots,k_{n-1})$, $i = \overline{1,n}$, f_i being linear functions with integer number coefficients. This "if possible" shows that substitutions are not always possible. But when they are we must make all possible substitutions.

Note 1. The former algorithm can be easily introduced into a computer program.

Note 2. The former algorithm is more "rapid" than that of W. Sierpinski's 1, i.e., the general integer solution is reached after a smaller number of iterations (or, at least, the same) for any linear equation (2). In the first place, both aim at obtaining the coefficient ± 1 for at least one unknown variable. While Sierpinski started only by chance, decomposing the greatest coefficient in the module (writing it under the form of a sum between a multiple of the following smaller coefficient (in the module) and the rest), in our algorithm this decomposition is not accidental but always seeks the smallest $|r|$ and also chooses the coefficients a_i and a_j for which this minimum is achieved. That is, we test from the beginning the shortest way to the general integer solution. Sierpinski does not attempt to find the shortest way; he knows that his will take him to the general integer solution of the equation and is not interested in how long it will take. However, when an algorithm is introduced into a computer, program it is preferable that the process time should be as short as possible

Example 1

Let us solve in $\mathbf{Z}^3$ the equation: $17x - 7y + 10z = -12$

... We apply the former algorithm.

1. $h = 1,\ p = 1$
2. $r = 3,\ i = 3,\ j = 2$
3. $|3| \neq 1$ go on to step 4.
4. (1)

$$y = t_1 - \frac{10-3}{-7} \cdot z = t_1 + z$$

5. Assign $y := t_1$ $\qquad h := 2$

$a_3 := 3 \qquad p := 2$

with the other coefficients and variables remaining unchanged, go back to step 2.

2. $r = -1,\ i = 1,\ j = 3$

3. $|-1| = 1$

$x = -1(-3t_2 - (-7t_1) - 12) = 3t_2 - 7t_1 - 12$

$z = -1(17t_2 + (-7t_1) \cdot \frac{17-(-1)}{3} + \frac{-1-17}{3}(-12)) =$

$= -17t_2 + 42t_1 - 72$

(A) We substitute the values of x and z thus determined into the only statement (p) we have:

(1) $y = t_1 + z = --17t_2 + 43t_1 - 72$

(B) The substitution is not possible.

(C) The substitution is not possible.

(D) The general integer solution of the equation is:

$$\begin{cases} x = 3_{k_1} - 7k_2 + 12 \\ y = -17k_1 + 43k_2 - 72 \\ z = -17k_1 + 42k_2 - 72; \qquad k_1, k_2 \in \mathbf{Z} \end{cases}$$

References:

[1] Sierpinski, W.-- Ce știm și ce nu știm despre numerele prime?, Editura științifică, Bucharest, 1966.

[2] Creangă, I., Cazacu, C.,Mihuț, P., Opaiț, Gh.,Corina Reischer--Introducere în teoria numerelor, Ed. did. și ped., Bucharest, 1965.

[3] Popovici, C.P.--Aritmetica și teoria numerelor, Ed. did. și ped., Bucharest, 1963.

[4] Smarandache, Florentin---Un algorithm de rezolvare în numere întregi a ecuațiilor liniare.

INTEGER NUMBER SOLUTIONS OF LINEAR SYSTEMS

Definitions and Properties of the Integer Solution of a Linear System

Let $\sum_{j=1}^{n} a_{ij}x_j = b_i,\ i = \overline{1,m}$ (1)

a linear system with all coefficients being integer numbers (the case with rational coefficients is reduced to the same).

Definition 1. $x_j = x_j^o,\ j = \overline{1,n}$ is a particular integer solution of (1) if $x_j^o \in \mathbf{Z},\ j = \overline{1,n}$ and $\sum_{j=1}^{n} a_{ij}x_j^o = b_i,\ i = \overline{1,m}$.

Let the functions be $f_j : \mathbf{Z}^h \to \mathbf{Z},\ j = \overline{1,n}$ where $h \in \mathbf{N}^*$.

Definition 2. $x_j = f_j(k_1,\dots,k_h),\ j = \overline{1,n}$ is the general integer solution for (1) if:

(a) $\sum_{j=1}^{n} a_{ij}f_j(k_1,\dots,k_h) = b_i,\ i = \overline{1,m}$, irrespective of $(k_1,\dots,k_h) \in \mathbf{Z}$;

(b) Irrespective of $x_j = x_j^o,\ j = \overline{1,n}$ a particular integer solution of (1), there is $(k_1^o,\dots,k_h^o) \in \mathbf{Z}$ so that $f_j(k_1^o,\dots,k_h^o) = x_j,\ j = \overline{1,n}$

(In other words, the general solution is the solution that comprises all the other solutions.)

Property 1

A general solution of a linear system of m equations with n

unknowns, $r(A) = m < n$, is undetermined $n - m$ times.

Proof:

We assume by reductio ad absurdum that it is of order r, $1 \le r \le n - m$ (the case $r = 0$, i.e., when the solution is particular, is trivial). It follows that the general solution is of the form:

$$(S_1) \qquad \begin{cases} x_1 = u_{11}p_1 + \ldots + u_{1r}p_r + v_1 \\ \vdots \\ x_n = u_{n1}p_1 + \ldots + u_{nr}p_r + v_n;\ u_{ih},\ \forall i \in \mathbf{Z} \\ p_h = \text{parametres } \in \mathbf{Z} \end{cases}$$

We prove that the solution are undetermines $n - m$ times

The homogenous linear system (1), solved in r has the solution:

$$\begin{cases} x_1 = \dfrac{D^1_{m+1}}{D} x_{m+1} + \ldots + \dfrac{D^1_n}{D} x_n \\ \qquad\vdots \\ x_m = \dfrac{D^m_{m+1}}{D} x_{m+1} + \ldots + \dfrac{D^m_n}{D} x_n \end{cases}$$

Let $x_i = x_i^o$, $i = \overline{1,n}$, be a particular solution of the linear system (1).

Considering

$$\begin{cases} x_{m+1} = D \cdot k_{m+1} \\ \vdots \\ x_n = D \cdot k_n \end{cases}$$

we get a solution

$$\begin{cases} x_1 = D^1_{m+1}k_{m+1}+\ldots+D^1_n k_n + x^o_1 \\ \vdots \\ x_m = D^m_{m+1}k_{m+1}+\ldots+D^m_n k_n + x^o_m \\ x_{m+1} = D\cdot k_{m+1} + x^o_{m+1} \\ \vdots \\ x_n = D\cdot k_n + x^o_n,\ k_j = \text{parameters} \in \mathbf{Z} \end{cases}$$

which depends on the $n-m$ independent parameters, for the system (1). Let the solution be undetermined $n-m$ times:

$$(S_2) \qquad \begin{cases} x_1 = c_1 k_1+\ldots+c_{1n-m}k_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1}k_1+\ldots+c_{nn-m}k_{n-m} + d_n \\ c_{ij},\ d_i \in Z,\ k_j = \text{parameters} \in \mathbf{Z} \end{cases}$$

(There are such solutions, we have proven it before.) Let the system be:

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1+\ldots+a_{mn}x_n = b_m \end{cases}$$

x_i = unknowns $\in \mathbf{Z}$, $a_{ij}, b_i \in \mathbf{Z}$

I. The case $b_i = 0,\ i = \overline{1,m}$ results in a homogenous linear system:

$a_{i1}x_i+\ldots+a_{in} = 0,\ i = \overline{1,m}$.

$$(S_2) \Rightarrow \quad a_{i1}(c_{i1}k_1+\ldots+c_{1n-m}k_{n-m} + d_1)+\ldots+$$
$$+a_{in}(c_{n1}k_1+\ldots+c_{nn-m}k_{n-m} + d_n) = 0$$
$$0 = (a_{i1}c_{11}+\ldots+a_{in}c_{n1})k_1+\ldots+(a_{i1}c_{1n-m}+\ldots+$$
$$a_{in}c_{nn-m})\cdot k_{n-m}+(a_{i1}d_1+\ldots+a_{in}d_n),\ \forall k_j \in \mathbf{Z}$$

For $k_1 =\ldots= k_{n-m} = 0 \Rightarrow a_{i1}d_1+\ldots+a_{in}d_n = 0$.

For $k_1 =\ldots= k_{h-1} = k_{h+1} =\ldots= k_{n-m} = 0$ and $k_h = 1 \Rightarrow$

$$\Rightarrow (a_{i1}c_{ih}+\ldots+a_{in}c_{nh}) + (a_{i1}d_1+\ldots+a_{in}d_d^{(n)}) = 0 \Rightarrow$$

$a_{i1}c_{1h}+\ldots+a_{in}c_{nh} = 0$, $\forall i = \overline{1,m}$, $\forall h = \overline{1,n-m}$.

Vect. $V_h = \begin{pmatrix} c_{1h} \\ \vdots \\ \vdots \\ c_{nh} \end{pmatrix}$, $h = \overline{1,n-m}$ are the particular solutions of the system.

V_h, $h = \overline{1,n-m}$ also lineary independent because the solution is undetermined $n-m$ times $\{V_1,\ldots,V_{n-m}\}+d$ is a linear variety that includes the solutions of the sistem obtaiend from (S_2) Similarly, for (S_1) we deduce that $U_s = \begin{pmatrix} U_{1s} \\ \vdots \\ U_{ns} \end{pmatrix}$, $s = \overline{1,r}$ are particular solutions of the given system and are linearly independent, because (S_1) is undetermined times, and

$V = \begin{pmatrix} V_1 \\ \vdots \\ V_n \end{pmatrix}$ is a solution of the given sistem.

The case (a) $U_1,\ldots,U_r$, V = linearly dependent, it follows that $\{U_1,\ldots,U_r\}$ is a free submodule of order $r < n-m$ of solutions of the given system, then, it follows that there are solutions that belong to $\{V_1,\ldots,V_{n-m}\}+d$ and which do not belong to $\{U_1,\ldots,U_r\}$, a fact which contradicts the assumption that (S_1) is the general solution.

The case (b). $U_1,\ldots,U_r$, V = linearly independent.

$\{U_1,\ldots,U_r\}+V$ is a linear vatiety that comprises the solutions of the given system, which were obtained from (S_1) It follows

that the solution belongs $\{V_1,\dots,V_{n-m}\}+d$ and does not belong to $\{U_1,\dots,U_r\}+V$, a fact wich is a contradiction to the assumption that (S_1) is the general solution.

II. When there is an $i\in\overline{1,m}$, with $b_i \neq 0 \Rightarrow$ nonhomogeneous linear system

$$a_{i1}x_1+\dots+a_{in}x_n = b_i,\ i=\overline{1,m}$$

$$(S_2)\ \Rightarrow a_{i1}(c_{11}k_1+\dots+c_{1n-m}k_{n-m}+d_1)+\dots+$$
$$+\ a_{in}(c_{n1}k_1+\dots+c_{nn-m}k_{n-m}+d_n)=b_i$$

it follows that

$$\Rightarrow (a_{i1}c_{11}+\dots+a_{in}c_{n1})k_1+\dots+(a_{i1}c_{1n-m}+\dots+a_{in}c_{nn-m})k_{n-m}+$$
$$+\ (a_{i1}d_1+\dots+a_{in}d_n)=b_i$$

for $k_1=\dots=k_{n-m}=0 \Rightarrow a_{i1}d_1+\dots+a_{in}d_n=b_i$;

for $k_1=\dots=k_{j-1}=k_{j+1}=\dots=k_{n-m}=0$ and $k_j=1\Rightarrow$

$\Rightarrow\ (a_{i1}c_{1j}+\dots+a_{in}c_{nj})+(a_{in}d_1+\dots+a_{in}d_n)=b_i$ it follows that

$$\begin{cases} a_{i1}c_{1j}+\dots+a_{in}c_{nj}=0 \\ a_{i1}d_1+\dots+a_{in}d_n=b_i \end{cases};\ \forall\ i=\overline{1,m},\ \forall\ j=\overline{1,n-m}$$

$V_j=\begin{pmatrix} c_{1j} \\ \vdots \\ c_{nj}\end{pmatrix}$, $j=\overline{1,n-m}$, are linearly independent because the solution (S_2) is undetermined $n-m$ times.

?! V_j, $j=\overline{1,n-m}$, and $d=\begin{pmatrix} d_1 \\ \vdots \\ d_n\end{pmatrix}$ are linearly independent.

We assume that they are not linearly independent. It follows that

---

"?!" means "to prove that"

$$d = s_1 V_1 + \ldots + s_{n-m} V_{n-m} = \begin{pmatrix} s_1 c_{11} + \ldots + s_{n-m} c_{1n-m} \\ \vdots \\ s_1 c_{n1} + \ldots + s_{n-m} c_{nn-m} \end{pmatrix}$$

Irrespective of $i = \overline{1,m}$:

$$b_1 = a_{i1} d_1 + \ldots + a_{in} d_n = a_{i1}(s_1 c_{11} + \ldots + s_{n-m} c_{1n-m}) + \\ + \ldots + a_{in}(s_1 c_{n1} + \ldots + s_{n-m} c_{nn-m}) = (a_{i1} c_{11} + \ldots + \\ + a_{in} c_{n1}) s_1 + \ldots + (a_{i1} c_{1n-m} + \ldots + a_{in} c_{nn-m}) s_{n-m} = 0.$$

Then, $b_i = 0$, irrespective of $i = \overline{1,m}$, contradicts the hypothesis (that there is an $i \in \overline{1,m}$, $b_i \neq 0$). It folows that $V_1, \ldots, V_{n-m}$, d are lineary independent.

$\{V_1, \ldots, V_{n-m}\} + d$ d is a linear variety that contains the solutions of the nonhomogeneous system, solutions obtained from (S_2). Similarly it follows that $\{G_1, \ldots, G_r\} + V$ is a linear variety containing the solutions of the nonhomogeneous system, obtaiend from (S_1).

$n - m > r$ it follows that there are solutions of the system that belong to ($\{V_1, \ldots, V_{n-m}\} + d$ and which do not belong to $\{G_1, \ldots, G_r\} + V$ this contradicts the fact that (S_1) is the general solution). Then, it shews that the general solution depends on the $n - m$ independent parameters.

Theorem 1. The general solution of a nonhomogeneous linear system is equal to the general solution of an associated linear system plus a particular solution of the nonhomogeneous system.

Proof:

Let the homogeneous linear solution:

$$\begin{cases} a_{11} x_1 + \ldots + a_{1n} x_n = 0 \\ \vdots \\ a_{m1} x_1 + \ldots + a_{mn} x_n = 0 \end{cases}, \ (AX = 0)$$

with the general solution:

$$\begin{cases} x_1 = c_1 k_1 + \ldots + c_{1n-m} k_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1} k_1 + \ldots + c_{nn-m} k_{n-m} + d_n \end{cases},$$

and $\begin{cases} x_1 = x_1^o \\ \vdots \\ x_n = x_n^o \end{cases}$ with the general solution:

a particular solution of the nonhomogeneous linear system $AX = b$;

$$?! \begin{cases} x_1 = c_1 k_1 + \ldots + c_{1n-m} k_{n-m} + d + x_1^o \\ \vdots \\ x_n = c_{n1} k_1 + \ldots + c_{nn-m} k_{n-m} + d_n + x_n^o \end{cases}$$

is a solution of the nonhomogeneous linear system.

We have written

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix},\ X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},\ b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix},\ 0 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

(vector of dimension m),

$$K = \begin{pmatrix} k_1 \\ \vdots \\ k_{n-m} \end{pmatrix},\ C = \begin{pmatrix} c_{11} \ldots c_{1n-m} \\ \vdots \\ c_{n1} \ldots c_{nn-m} \end{pmatrix},\ d = \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix},\ x^o = \begin{pmatrix} x_1^o \\ \vdots \\ x_n^o \end{pmatrix};$$

$$AX = A(Ck + d + x^o) = A(Ck + d) + AX^o = b + 0 = b$$

We will prove that irrespective of $x_1 = y_1^o$

$\vdots$

$x_n = y_n^o$

there is a particular solution of the nonhomogeneous sistem

$$\begin{cases} k_1 = k_1^o \in \mathbf{Z} \\ \vdots \\ k_{n-m} = k_{n-m}^o \in \mathbf{Z} \end{cases}$$, with the proper ty:

$$\begin{cases} x_1 = c_{11}k_1^o + \ldots + c_{1n}k_{n-m}^o + d_1 + x_1^o = y_1^o \\ \vdots \\ x_n = c_{n1}k_1^o + \ldots + c_{nn-m}k_{n-m}^o + d_1 + x_n^o = y_n^o \end{cases}$$

We write $Y^o = \begin{pmatrix} y_1^o \\ \vdots \\ y_n^o \end{pmatrix}$

We demonstrate that those $k_j^o \in \mathbf{Z}$, $j = \overline{1, n-m}$ are those for which $A(CX^o + d) = 0$ (there are such $X_j^o \in \mathbf{Z}$ because

$$\begin{cases} x_1 = 0 \\ \vdots \\ x_n = 0 \end{cases}$$

is a particular solution of the homogenous linear system and $X = CK + d$ is a general solution of the nonhomogeneous linear system) $A(CK^o + d + X^o - Y^o) = A(CK^o + d) + AX^o - AY^o =$ $= 0 + b - b = 0$.

Property 2. The general solution of homogenous linear system can be written under the form:

(SG)

(2) $$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1\,n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{n\,n-m}k_{n-m} \end{cases}$$

$k_j = a$ parameter belonging to Z (with $d_1 = d_2 = \ldots = d_n = 0$).

Proof:

(SG) = general solution. It results that (SG) is undetermined $(n-m)$ times.

Let (SG) be of the form

$$\begin{cases} x_1 = c_{11}p_1 + \ldots + c_{1n-m}p_{n-m} + d_1 \\ \vdots \\ x_n = c_{n1}p_1 + \ldots + c_{nn-m}p_{n-m} + d_n \end{cases}$$

with not all $d_i = 0$; we demonstrate that it can be written under the form (2); the system has the trivial solution

$$\begin{cases} x_1 = 0 \in \mathbf{Z} \\ \vdots \qquad\qquad ; \\ x_n = 0 \in \mathbf{Z} \end{cases}$$

it results that there are $p_j \in \mathbf{Z}$, $j = \overline{1, n-m}$,

$$(4) \begin{cases} x_1 = c_{11}p_1^o + \ldots + c_{1n-m}p_{n-m}^o + d_1 = 0 \\ \vdots \\ x_n = c_{n1}p_1^o + \ldots + c_{nn-m}p_{n-m}^o + d_n = 0 \end{cases}$$

Substituting $p_j = k_j + p_j^o$, $j = \overline{1, n-m}$, in (3)

$$\left.\begin{matrix} k_j \in \mathbf{Z} \\ p_j^o \in \mathbf{Z} \end{matrix}\right\} \Rightarrow p_j \in \mathbf{Z}$$

$$\left.\begin{matrix} p_j \in \mathbf{Z} \\ p_j^o \in \mathbf{Z} \end{matrix}\right\} \Rightarrow k_j = p_j - p_j^o \in \mathbf{Z}$$

which means that they do not make any restrictions.

It results that

$$\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} + (c_{11}p_1^o + \ldots + c_{1n-m}p_{n-m}^o + d_1) \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} + (c_{n1}p_1^o + \ldots + c_{nn-m}p_{n-m}^o + d_n) \end{cases}$$

But $c_{h1}p_1^o+\ldots+c_{hn-m}p_{n-m}^o + d_h = 0$, $h=\overline{1,n}$, (from (4))
Then the general solution is of the form:

$$\begin{cases} x_1 = c_{11}k_1+\ldots+c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1+\ldots+c_{nn-m}k_{n-m} \end{cases}$$

k_j = parameters $\in \mathbf{Z}$, $j=\overline{1,n-m}$; it results that
$d_1 = d_2 = \ldots = d_n = 0$.

Theorem 2. Let the homogenous linear system be:

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1+\ldots+a_{mn}x_n = 0, \qquad r(A)=m \end{cases}$$

$(a_{h1},\ldots,a_{hn}) = 1$, $h=\overline{1,m}$ and the general solution

$$\begin{cases} x_1 = c_{11}k_1+\ldots+c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1+\ldots+c_{nn-m}k_{n-m} \end{cases}$$

then $(a_{h1},\ldots,a_{hi-1},a_{hi+1},\ldots,a_{hn}) | (c_{i1},\ldots,c_{in-m})$
irrespective of $h=\overline{1,m}$ and $i=\overline{1,n}$.

Proof:

Let some arbitrary be $h\in\overline{1,m}$ and some arbitrary $i\in\overline{1,n}$; $a_{h1}x_1+\ldots+a_{hi-1}x_{i-1} + a_{hi+1}x_{i+1}+\ldots+a_{hn}x_n = a_{hi}x_i$. Because $(a_{h1},\ldots,a_{hi-1},a_{hi+1},\ldots,a_{hn}) | a_{hi}$ it results that $d=(a_{h1},\ldots,a_{hi-1},a_{hi+1},\ldots,a_{hn}) | x_i$ irrespective of the value of x_i in the vector of particular solutions; for $k_2 = k_3 = \ldots = k_{n-m} = 0$ and $k_1 = 1$ we get the particular solution:

$$\begin{cases} x_1 = c_{11} \\ \vdots \\ x_i = c_{i1} \Rightarrow d | c_{i1} \\ \vdots \\ x_n = c_{n1} \end{cases}$$

For $k_1 = k_2 = \ldots = k_{n-m-1} = 0$ and $k_{n-m} = 1$ the following particular solution results:

$$\begin{cases} x_1 = c_{1n-m} \\ \vdots \\ x_i = c_{in-m} \\ \vdots \\ x_n = c_{nn-m} \end{cases}$$

it results that $d | c_{in-m}$; hence $d | c_{ij}$, $j = \overline{1, n-m}$ $\Rightarrow$ $d | (c_{i1}, \ldots, c_{in-m})$.

Theorem3.

If $\begin{cases} x_1 = c_{11}k_1 + \ldots + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c_{nn-m}k_{n-m} \end{cases}$

k_j = parameters $\in \mathbf{Z}$, $c_{ij} \in \mathbf{Z}$ being given,

is the general solution of the homogenous linear system

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = 0, \qquad r(A) = m < n \end{cases}$$

then $(c_{1j}, \ldots, c_{nj}) = 1$, $\forall\ j = \overline{1, n-m}$.

Proof:

We assume, by reductio ad absurdum, that there is

$j_o \in \overline{1, n-m}$: $(c_{1j_o}, \ldots, c_{nj_o}) = d$ we consider the maximal co-divisor > 0; we reduce the case when the maximal co-divisor is $-d$ to the case when it is equal to d (nonrestrictive hypothesis); then the general solution can be written under the form:

$$(5)\begin{cases} x_1 = c_{11}k_1 + \ldots + c'_{1j_o} dk_{j_o} + \ldots + c_{1n-m}k_{n-m} \\ \vdots \\ x_n = c_{n1}k_1 + \ldots + c'_{nj_o} dk_{j_o} + \ldots + c_{nn-m}k_{n-m} \end{cases}$$

where $d = (c_{ij_o}, \ldots, c_{nj_o})$, $c_{ij_o} = d \cdot c'_{ij_o}$ and $(c'_{ij_o}, \ldots, c'_{nj_o}) = 1$.

We demonstrate that

$$\begin{cases} x_1 = c'_{1j_o} \\ \vdots \\ x_n = c'_{nj_o} \end{cases}$$

is a particular solution of the homogenous linear system.
We write

$$C = \begin{pmatrix} c_{11} & \cdots & c'_{ij_o} & d & \cdots & c_{1n-m} \\ \vdots & & \vdots & & & \vdots \\ c_{n1} & \cdots & c_{nj_o} & d & \cdots & c_{nn-m} \end{pmatrix}, k = \begin{pmatrix} k_1 \\ \vdots \\ k_{j_o} \\ \vdots \\ k_{n-m} \end{pmatrix}$$

$x = c \cdot k$ the general solution.

We know $AX = 0 \Rightarrow A(CK) = 0$, $A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \\ a_{n1} & \cdots & a_{mn} \end{pmatrix}$

We assume that the principal variables are $x_1, \ldots, x_m$ (if not, we have to renumber). It follows that $x_{m+1}, \ldots, x_n$ is the secondary variables.

For $k_1 = \ldots = k_{j_o - 1} = k_{j_o + 1} = \ldots = k_{n-m} = 0$ and $k_{j_o} = 1$ we get a particular solution of the system

$$\begin{cases} x_1 = c'_{1j_o} d \\ \vdots \\ x_n = c'_{nj_o} d \end{cases} \Rightarrow 0 = A\begin{pmatrix} c'_{1j_o} d \\ \vdots \\ c'_{nj_o} d \end{pmatrix} = d \cdot A\begin{pmatrix} c'_{1j_o} \\ \vdots \\ c'_{nj_o} \end{pmatrix} \Rightarrow A\begin{pmatrix} c'_{1j_o} \\ \vdots \\ c'_{nj_o} \end{pmatrix} = 0$$

$$\Rightarrow \begin{cases} x_1 = c'_{1j_o} \\ \vdots \\ x_n = c'_{nj_o} \end{cases}$$

is the particular solution of the system.

We demonstrate that this particular solution cannot be obtained by

$$(6) \begin{cases} x_1 = c_1 k_1 + \ldots + c'_{1j_o} dk_{j_o} + \ldots + c_{1n-m} k_{n-m} = c'_{1j_o} \\ \vdots \\ x_n = c_{n1} k_1 + \ldots + c'_{nj_o} dk_{j_o} + \ldots + c_{nn-m} k_{n-m} = c'_{nj_o} \end{cases}$$

$$(7) \begin{cases} x_{m+1} = c_{m+1} k_1 + \ldots + c'_{m+1} dk_{j_o} + \ldots + c_{m+1,n-m} k_{n-m} = c'_{m+1j_o} \\ \vdots \\ x_n = c_{n1} k_1 + \ldots + c'_{nj_o} dk_{j_o} + \ldots + c_{nn-m} k_{n-m} = c'_{nj_o} \end{cases}$$

$$\Rightarrow \qquad k_{j_o} = \frac{\begin{vmatrix} c_{m+1,1} & \cdots & c_{m+1j} & \cdots & c_{m+1,n-m} \\ \vdots & & \vdots & o. & \vdots \\ c_{h1} & \cdots & c_{nj} & \cdots & c_{n,n-m} \end{vmatrix}}{\begin{vmatrix} c_{m+1,1} & \cdots & c'_{m+1j_o} d & \cdots & c_{m+1,n-m} \\ \vdots & & \vdots & o. & \vdots \\ c_{h1} & \cdots & c'_{nj} d & \cdots & c_{n,n-m} \end{vmatrix}} = \frac{1}{d} \notin \mathbf{Z}$$

(because $d \neq 1$).

It is important to out the fact that those $k_j = k_j^o$, $j = \overline{1, n-m}$, that satisfy system (7) also satisfy system (6), because, otherwise (6) would not satisfy the definition of the

solution of a linear system of equations (i.e., considering system (7) the hypothesis was not restrictive). From $X_{j_o} \in \mathbf{Z}$ follows that (6) is not the general solution of the homogenous linear system contrary to the hypothesis); then $(c_{1j},\dots,c_{nj}) = 1$, irrespective of j $j = \overline{1, n-m}$.

Propriety 3. Let the linear system be

$$\begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1 + \dots + a_{mn}x_n = b_m \end{cases}$$

$a_{ij},\ b_i \in \mathbf{Z},\ r(A) = m < n,\ x_j =$ unknowns $\in \mathbf{Z}$.

Solves in R, we get

$$\begin{cases} x_1 = f_1(x_{m+1},\dots,x_n) \\ \vdots \\ x_m = f_m(x_{m+1},\dots,x_n) \end{cases}$$; $x_1,\dots,x_m$ are the main variables,

where f_i are linear functions of the form:

$f_i = \dfrac{c^i_{m+1}x_{m+1} + \dots + c^i_n x_n + e_i}{d_i}$ where $c^i_{m+j},\ d_i,\ e_i \in \mathbf{Z}$; $i = \overline{1, m},\ j = \overline{1, n-m}$.

If $\dfrac{e_i}{d_i} \in \mathbf{Z}$ irrespective of $i = \overline{1, m}$ then the linear system has integer solution.

Proof:

For $1 \le i \le m$, $x_i \in \mathbf{Z}$, then $f_j \in \mathbf{Z}$. Let:

$$\begin{cases} x_{m+1} = u_{m+1}k_{m+1} \\ \vdots \\ x_n = u_n k_n \\ \vdots \\ x_1 = v_{m+1}^1 k_{m+1} + \ldots + v_n^1 k_n + \dfrac{e_1}{d_1} \\ \vdots \\ x_m = v_{m+1}^m k_{m+1} + \ldots + v_n^m k_n + \dfrac{e_m}{d_m} \end{cases}$$

be a solution, where u_{m+1} is the maximal co-divisor of the denominators of the fractions $\dfrac{c_{m+j}^i}{d_i}$, $i = \overline{1,m}$, $j = \overline{1,n-m}$ calculated after their complete simplification.

$v_{m+j}^i = \dfrac{c_{m+j}^i u_{m+j}}{d_i} \in \mathbf{Z}$ this is a solution undetermined n-m times depends on $n-m$ indepedent parameters: $(k_{m+1},\ldots,k_n)$ but is not a general solution.

Property 4. Under the conditions of property 3, if there is an $i_o \in \overline{1,m}$: $f_{i_o} = u_{m+1}^{i_o} x_{m+1} + \ldots + u_n^{i_o} x_n + \dfrac{e_{i_o}}{d_{i_o}}$ with $u_{m+j}^{i_o} \in \mathbf{Z}$, $j = \overline{1,n-m}$, and $\dfrac{e_{i_o}}{d_{i_o}} \notin \mathbf{Z}$ then the system does not have integer solution.

Proof:

$\forall x_{m+1},\ldots,x_n$ in $\mathbf{Z}$, it results in $x_{i_o} \notin \mathbf{Z}$.

Theorem 4. Let the linear system be

$$\begin{cases} a_{11}x_1+\ldots+a_{1n}x_n = b_1 \\ \vdots \\ a_{m1}x_1+\ldots+a_{mn}x_n = b_m \end{cases}$$

$a_{ij}, b_i \in \mathbf{Z}$, x_j = unknowns $\in \mathbf{Z}$, $r(A) = m < n$. If there are indices $1 \le i_1 < \ldots < i_m \le n$, $i_h \in \{1,2,\ldots,n\}$, $h = \overline{1,m}$, with the property:

$$\Delta = \begin{vmatrix} a_{1i_1} & \ldots & a_{1i_m} \\ \vdots & & \vdots \\ a_{mi_1} & & a_{mi_m} \end{vmatrix} \neq 0 \text{ and}$$

$$\Delta_{x_{i_1}} = \begin{vmatrix} b_1 & a_{1i_2} & \ldots & a_{1i_m} \\ \vdots & \vdots & & \vdots \\ b_m & a_{mi_2} & \ldots & a_{mi_m} \end{vmatrix} \text{ is divided by } \Delta$$

.

.

.

$$\Delta_{x_{i_m}} = \begin{vmatrix} a_{1i_1} & a_{1i_{m-1}} & \ldots & b_1 \\ \vdots & \vdots & & \vdots \\ a_{mi_1} & a_{mi_{m-1}} & \ldots & b_m \end{vmatrix} \text{ is divided by } \Delta$$

then the system has integer number solutions.

Proof:

We use property 3

$d_i = \Delta$, $i = \overline{1,m}$; $e_{i_h} = \Delta_{x_{i_h}}$, $h = \overline{1,m}$.

Note 1. It is not true in the reverse case

Consequence 1. Any homogenous linear system has integer number solutions (besides the trivial one); $r(A) = m < n$.

Proof:

$\Delta_{x_{i_h}} = 0 : \Delta$, irrespective of $h = \overline{1,m}$.

Consequence 2. If $\Delta = \pm 1$, it follows that the linear system has integer number solutions.

Proof:

$\Delta_{x_{i_h}} :(\pm 1)$, irrespective of $h = \overline{1,m}$;

$\Delta_{x_{i_h}} \in \mathbf{Z}$.

FIVE INTEGER NUMBER ALGORITHMS TO SOLVE LINEAR SYSTEMS

This chapter further extends the results obtained in 4 and 5 (from linear equation to linear systems). Each algorithm is thoroughly demonstrated and then an example is given.

Five integer number algorithms to solve linear systems are further given.

Algorithm 1 (method of substitution)

(Although simple, this algorithm requires complex calculus but is, nevertheless, easy to adapt to a computer program).

Some integer number equation are initially solved (which is usually simpler) by means of one of the algorithms 4 or 5. (If there is an equation of the system which does not have integer systems, then the integer system does not have integer systems. Stop.) The general integer solution of the equation will depend on n-1 integer number parameters (see 5):

(p_1) $\quad x_{i_1} = f_{i_1}^{(1)}(k_1^{(1)},\dots,k_{n-1}^{(1)})$, $\; i=\overline{1,n}$, where all the functions $f_{i_1}^{(1)}$ are linear and have integer number coefficients.

This general integer number system (p_1) is introduced into the other $m-1$ equations of the system. We get a new system of $m-1$ equations with $n-1$ unknown variables:

$k_{i_1}^{(1)}$, $i_1=\overline{1,n-1}$, which is also to be solved with integer numers. The procedure is similar. Solving a new equation, we obtain its general integer solution:

(p_2) $\quad k_{i_2}^{(1)} = f_{i_2}^{(2)}(k_1^{(2)},\dots,k_{n-2}^{(2)})$, $i_2=\overline{1,n-1}$,

where all the functions $f_{i_2}^{(2)}$ are linear, with integer number coefficients. (If, along this algorithm we come across an

equation which does not have integer solutions, then, the initial system does not have integer solution. Stop.)

In the case that all the solved equations had integer system at step (j), $1 \le j \le r$ (r being of the same rank as the matrix associated to the system) then:

$$(p_j) \quad k_{i_j}^{(j-1)} = f_{i_j}^{(j)}(k_1^{(j)},\ldots,k_{n-j}^{(j)}),\ i_j = \overline{1, n-j+1},$$

$f_{i_j}^{(j)}$ are linear functions and have integer number coefficients.

Finally, after r steps, and if all the solved equations had integer solutions, we get to the integer solution of one equation with n-r+1 unknown variables.

The system will have integer solutions if an only in this last equation has integer solutions. If it does, let the general integer solution of it be:

$$(p_r) \quad k_{i_r}^{(r-1)} = f_{i_r}^{(r)}(k_1^{(r)},\ldots,k_{n-1}^{(r)}),\ i_r = \overline{1, n-r+1},$$

where all $f_{i_r}^{(r)}$ are linear functions with integer number coefficients.

Now the reverse procedure follows.

We introduce the values of $k_{i_r}^{(r-1)}$, $i_r = \overline{1, n-r+1}$, at step p_r in the values of $k_{i_{(r-1)}}^{(r-2)}$, $i_{r-1} = \overline{1, n-r+2}$ from step (p_{r-1}).

It follows:

$$k_{i_{r-1}}^{(r-2)} = f_{i_{r-1}}^{(r-1)}(f_1^{(r)}(k_1^{(r)},\ldots,k_{n-r}^{(r)}),\ldots,f_{n-r+1}^{(r)}(k_1^{(r)},\ldots,k_{n-r}^{(r)})) =$$
$$= g_{i_{r-1}}^{(r-1)}(k_1^{(r)},\ldots,k_{n-r}^{(r)}),\ i_{r-1} = \overline{1, n-r-1},$$

from which it follows that $g_{i_r}^{(r-1)}$ are linear functions with integer number coefficients.

Then follow those from (p_{r-2}) in (p_{r-e}) and so on, until we introduce the values obtained at step (p_2) in those from the step (p_1). It will follow:

$x_{i_1} = g_i^{(1)}(k_1^{(r)},\ldots,k_{n-r}^{(r)})$ **notation** $g_{i_1}(k_1,\ldots,k_{n-r})$, $i = \overline{1,n}$,

with all g_{i_1} most obviously, linear functions with integer number coefficients (the notation was made for simplicity and aesthetical aspects). This is, thus, the general integer solution, of the initial system.

The correctness of algorithm 1. The algorithm is finite because it has r steps on the first way and $r-1$ steps on the reverse. ($r < +\infty$). Obviously, if one equation of one system does not have (integer number) solutions then the system does not have solutions either.

Writing S for the initial system and S_j the system resulted from step (p_j), $1 \le j \le r-2$ it follows that passing from (p_j) to (p_{j+1}) we pass from a system S_j to a system S_{j+1} equivalent from the viewpoint of the integer number solution, i.e., $k_{i_j}^{(j-1)} = t_{i_j}^{o}$, $i_j = \overline{1,n-j+1}$, which is a particular integer solution of the system S_j if and only $k_{i_{j+1}}^{(j)} = h_{i_{j+1}}^{o}$, $i_{j+1} = \overline{1,n-j}$, is a particular integer solution of the system S_{j+1} where $k_{i_{j+1}}^{o} = f_{i_{j+1}}^{(j+1)}(t_1^{o},\ldots,t_{n-j+1}^{o})$, $i_{j+1} = \overline{1,n-j}$. Hence, their general integer solutions are also equivalent (considering these substitutions). So that, in the end, the solving of the initial system S is equivalent with the solving of the equation (of the system consisting of one equation) S_{r-1} with integer numer coefficients. It follows that the system S has integer number solution if and only if the systems S_j have integer number solution, $1 \le j \le r-1$.

Example 1. By means of algorhythm 1, let us calculate the integer number solution of the system:

$$(S)\begin{cases} 5x-7y-2z+6w=6 \\ -4x+6y-3z+11w=0 \end{cases}$$

Solution: We solve the first integer number equation. We obtain the general integer soution (see [4] or [5]):

$$(p_1)\begin{cases} x=t_1+2t_2 \\ y=t_1 \\ z=-t_1+5t_2+3t_3-3 \\ w=t_3 \end{cases}$$

where $t_1, t_2, t_3 \in \mathbf{Z}$

Substituting in the second, we get the system:

$$(S_1)\ 5t_1-23t_2+2t_3+9=0$$

Solving this integer equation we obtain its general integer solution:

$$(p_2)\begin{cases} t_1=k_1 \\ t_2=k_1+2k_2+1 \\ t_3=9k_1+23k_2+7 \end{cases}$$

where $k_1, k_2 \in \mathbf{Z}$.

The reverse way. Substituting (p_2) in (p_1) we obtain:

$$\begin{cases} x=3k_1+4k_2+2 \\ y=k_1 \\ z=31k_1+79k_2+23 \\ w=9k_1+23k_2+7 \end{cases}$$

where $k_1, k_2 \in \mathbf{Z}$ which is the general integer solution of the initial system (S). Stop.

Algorithm 2

Input

A linear system (1) without all $a_{ij}=0$.

Output

We decide on the possibility of an integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. $t = 1$, $h = 1$, $p = 1$
2. (A) Divide each equation by the largest codivisor of the coefficients of the unknown variables. If you do not get an integer quotient for at least one equation, then the system does not have integer solutions.Stop.
   (B) If there is an inequality in the system, then the system does not have integer solutions. Stop.
   (C) If the repetition of more equations occurs, keep one and if an equation is an identity, remove it from the system.
3. If there is (i_o, j_o) so that $|a_{i_o j_o}| = 1$ then obtain the value of the variable x_{j_o} from equation i_o; statement (T_t). Substitute this statement (where possible) in the other equations of the system and in the statement (T_{t-1}), (H_h) and (P_p) for all i, h and p. Consider $t := t + 1$, remove equation (i_o) from the system. If there is not such a pair, go on to step 5.
4. Does the system (left) have at least one unknown variable? If it does, consider the new data and go on to step 2. If it does not, write the general integer solution of the system substituting $k_1, k_2, \ldots$ for all the variables fromthe right term of each expression which gives the value of the unknowns of the initial system, Stop.
5. Calculate $a = \min\limits_{i, j_1, j_2} \left\{ |r|, a_{ij_1} \equiv r (\bmod a_{ij_2}),\ 0 < |r| < |a_{ij_2}| \right\}$
   and determine the indices i, j_1, j_2 as wel as the r for which

this minimum can be calculated. (If there are more variables, choose one, arbitrarily.)

6. Write: $x_{j_2} = t_h \dfrac{a_{ij_1} - r}{a_{ij_2}} x_{ij_1}$, statement (H_h).

Substitute this statement (where possibile in all the equations of the system and in the statements (T_t), (H_h) and (P_p) for all t, h, and p.

7. (A) If $a \neq 1$, consider $x_{j_2} := t_h$, $h := h+1$, and go on to step 2.

(B) If $a=1$, then obtain the value of x_{j_1} from from the equation (i); statement (P_p).

Substitute this statement (where possible in the other equations of the system and in the relations (T_t), (H_h) and (P_{p-1}) for all t, h, and p.

Remove the equation (i) from the system.

Consider $h := h+1$, $p := p+1$, and go back to step 4.

The correctness of algorithm 2. Let the system (1) be.

Lemma 1. We consider the algorithm at step 5. Also, let
$M = \left\{|r|,\ a_{ij_1} \equiv r(\bmod a_{ij_2}), 0 < |r| < |a_{ij_2}|,\ i, j_1, j_2 = 1,2,3,\ldots\right\}$.
Then $M \neq \varnothing$.

Proof:

Obviously, M is finite and $M \subset N^*$. Then, M has a minimum if and only if $M \neq \varnothing$. We suppose, conversely, that $M = \varnothing$ Then $a_{ij_1} \equiv 0(\bmod a_{ij_2})$, $\forall i, j_1, j_2$. It follows as well that $a_{ij_2} \equiv 0(\bmod a_{ij_1}), \forall i, j_1, j_2$. That is $|a_{ij_1}| = |a_{ij_2}|$, $\forall i, j_1, j_2$. We consider an i_o arbitrary but fixed. It is clear that $(a_{i_o 1}, \ldots, a_{i_o n}) \sim a_{i_o j} \neq 0$, $\forall j$ (because the algorithm has passed

through the substeps 2(B) and 2(C)). But, as it has also passed through step 3, it follows that $|a_{i_o j}| \neq 1, \forall j$ but as it previously passed through step 2(A), it would result that $|a_{i_o j}| = 1, \forall j$. This contradiction shows that the assumption is false.

Lemma 2. Let $a_{i_o j_1} = r (\mathrm{mod}\, a_{i j_2})$ Substitute $x_{j_2} = t_h - \dfrac{a_{i_o j_1} - r}{a_{i_o j_2}} x_{j_1}$ in system (A) obtaining system (B), Then, $x_j = x_j^o,\ j = \overline{1,n}$ is the particular integer solution of (A) if and only if $x_j = x_j^o,\ j \neq j_2$ and $t_h = x_{j_2}^o - \dfrac{a_{i_o j_1} - r}{a_{i_o j_2}}$ is the particular integer solution of (B).

Lemma 3. Let $a_1 \neq$ and a_2 be obtained at step 5.
Then $0 < a_2 < a_1$
Proof:

It is sufficient to show that $a_1 < |a_{ij}|, \forall\ i, j$ because in order to get a_2 step 6 is obligatory, when the coefficients of the new system are calculated, a_1 being equal to a coefficient from the new system (equality of modules), yhe coefficient on $(i_o j_1)$.

Let $a_{i_o j_o}$ with the property $|a_{i_o j_o}| \leq a_1$. Hence, $a_1 \geq |a_{i_o j}| = \min\{|a_{i_o j}|\}$. Let $a_{i_o j_s}$ with $|a_{i_o j_s}| > |a_{i j_m}|$; there is such an element because $|a_{i_o j_m}|$ is the minimum of the coefficients in the module and not all $|a_{i_o j}|,\ j = \overline{1,n}$ are equal (conversely, it would result that $(a_{i_o j}, \ldots, a_{i_o n}) \sim a_{i_o j},\ \forall j \in \overline{1,r}$; the algorithm passed through substep 2(A) has simplified each

equation by the maximal co-divisor of its coefficients: hence, it would follow that $\left|a_{i_oj}\right| = 1$, $\forall j = \overline{1,n}$, which, again, cannot be real because the algorithm has also passe through step 3). Of the coefficients $a_{i_oj_m}$ we choose one with the propriety $a_{i_oj_{s_o}} \neq Ma_{i_oj_m}$ there is such an element (contrary, it would result $(a_{i_oj},\ldots,a_{i_on}) \sim \left|a_{i_oj_m}\right|$ but the algorithm has also passed through step 2(A) and it would men that $\left|a_{i_oj_m}\right| = 1$ which contradicts step 3 through which the algorithm has also passed).

Considering $q_o = \left[a_{i_oj_{s_o}} / a_{i_oj_m}\right] \in \mathbf{Z}$ and $r = a_{i_oj_{s_o}} - q_oa_{i_oj_m} \in \mathbf{Z}$, we have $a_{i_oj_{s_o}} \equiv r_o (\mathrm{mod}\, a_{i_oj_m})$ and $0 < \left|r_o\right| < \left|a_{i_oj_m}\right| < \left|a_{i_oj_o}\right| \leq a_1$. We have, thus, obtained an r_o with $\left|r_o\right| < a_1$, which is in contradiction with the very definition of a_1. Thus, $a_1 < \left|a_{ij}\right|$, $\forall\ i,j$.

Lemma 4. Algorithm 2 is finite.

Proof:

The functioning of the algorithm is meant to transform a linear system of m equations and n unknowns into one of $m_1 \times n_1$ with $m_1 < m$, $n_1 < n$ and, thus, successively into a final linear equation with $n - r + 1$ unknowns (where r is the rank of the associated matrix). This equation is solved by means of the same algorithm (which works as [5]). The general integer solution of the system will depend on the $n - 1$ integer number independent parameters (see [6]--similar proprieties can be established also the general integer solution of the linear system). The reduction of equations occurs at steps 2, 3 and substep 7(B). Steps 2 and 3 are obvious and, hence, trivial; they

can reduce the equations of the system (or even put an end to it) but only under particular conditions. The most important case finds its solution at step 7(B), which always reduces one equation of the system. As the number of equations is finite, we come to solve a single integer number equation. We also have to show that the transfer from one system $m_i \times n_i$ to another $m_{i+1} \times n_{i+1}$ is made in a finite interval of time: by steps 5 and 6 permanent substitution of variables are made until we to $a=1$ (we to $a=1$ because, according to lemma 3, all a-s are positive integer numbers and form a strictly decreasing row).

Theorem of correctness. Algorithm 2 correctly calculates the general integer solution of the linear system.

Proof:

Algorithm 2 is finite according to lemma 4. Steps 2 and 3 are obvious (see also [4], [5]). Their part is to simplify the calculations as much as possible . Step 4 tests the finality of the algorithm; the substitution with the parameters $k_1, k_2, \ldots$ has systemization and aesthetic reasons. The variables t, h, p are counter variables (started at step 1) and they are meant to count the statement of the type *T, H, P* (numering required by the substitutions at steps 3, 6 and substep 7(B); h also counts the new (auxiliary) variables introduced in the moment of decomposition of the system. The substitution from step 6 does not affect the general integer solution of the system (it follows from lemma 2). Lemma 1 shows that at step 5 there is always a, because $\varnothing \neq M \subset N^*$.

The algorithm performs the transformation of a system $m_i \times n_i$ into another, $a_{i+1} \times n_{i+1}$, equivalent to it, preserving the general solution (taking into account, however, the substitutions) (see also lemma 2).

Exemple 2. Calculate the integer solution of:

$$\begin{cases} -12x - 7y + 9z = 12 \\ \quad\quad - 5y + 8z + 10w = 0 \\ \quad\quad\quad\quad 0z + 0w = 0 \\ 15x \quad\quad + 21z + 69w = 3 \end{cases}$$

Solution:

We apply algorithm 2 (we purposely looked for an example to be passed through all the steps of this algorithm):

1. $t = 1,\ h = 1,\ p = 1$
2. (A) The fourth equation becomes: $5x + 7z + 23w = 1$

   (B) --

   (C) Equation 3 is removed.
3. No; go on to step 5.
5. $a = 2$ and $i = 1,\ j_1 = 2,\ j_2 = 3$, and $r=2$.
6. $z = t_1 + y$, the statement (H_1). Substituting it in the

$$-12x + 2y + 9t_1 \quad\quad = 12$$
$$3y + 9t_1 + 10w = 0$$
$$5x + 7y + 7t_1 + 23w = 1$$

7. $a \neq 1$ consider $z = t_1$, $h := 2$, and go back to step 2.

2. --
3. No. Step 5.
5. $a = 1$ and $i = 2,\ j_1 = 4,\ j_2 = 2$, and $r = 1$.
6. $y = t_2 - 3w$, the statement (H_2). Substituting in the system:

$$\begin{cases} -12x + 2t_2 + 9t_1 - 6w = 12 \\ \quad\quad 3t_2 + 8t_1 + w = 0 \\ 5x + 7t_2 + 7t_1 + 2w = 1 \end{cases}$$

   Substituting it in statement to (H_1), we get:

   $z = t_1 + t_2 - 3w$, statement $(H_1)'$.
7. $w = -3t_2 - 8t_1$ statement (P_1).

Substituting it in the system, we get:

$$\begin{cases} -12x + 20t_2 + 57t_1 = 12 \\ 5x + \quad t_2 - 9t_1 = 1 \end{cases}$$

Substituting it in the other statements, we get:

$z = 10t_2 + 25t_1$, $(H_1)''$;

$y = 10t_2 + 24t_1$, $(H_2)''$;

$h := 3$, $p := 2$, and go back to step 4.

4. Yes

2. --

3. $t_2 = 1 - 5x + 9t_1$, statement (T_1).

Substituting it (where possible) we get:

$\{-112x + 237t_1 = -8$ (the new system);

$z = 10 - 50x + 115t_1$, $(H_1)'''$

$y = 10 - 50x + 114t_1$, $(H_2)''$

$w = -3 + 15x - 35t_1$, $(P_1)'$

Consider $t := 2$ go on to step 4.

4. Yes. Go back to step 2. (From now on algorithm 2 works similarly with that from [5], with the only difference that the substitution must also be made in the statements obtained up to this point).

2. – –

3. No. Go on to step 5.

5. $a = 13$ (one three) and $i = 1$, $j_1 = 2$, $j_2 = 1$, and $r = 13$.

6. $x = t_3 + 2t_1$, statement (H_3).

After substitution we get:

$\{-112t_3 + 13t_1 = -8$ (the system)

$z = 10 - 50t_3 + 15t_1$, $(H_1)^{IV}$;

$y = 10 - 50t_3 + 14t_1, \quad (H_2)'''$;
$w = -3 + 15t_3 - 5t_1, \quad (P_1)''$;
$t_2 = 1 - 5t_3 - t_1, \quad (T_1)'$;

7. $x := t_3$, $h := 4$ and go on to step 2.

2. --
3. No, go on to step 5.
5. $a = 5$ and $i = 1$, $j_1 = 1$, $j_2 = 2$ and $r = 5$
6. $t_1 = t_4 + 9t_3$, statement (H_4).

Substituting it, we get: $5t_3 + 13t_4 = -8$ (the system).

$z = 10 + 85t_3 + 15t_4, \quad (H_1)^V$;
$y = 10 + 76t_3 + 14t_4, \quad (H_2)^{IV}$;
$x = 19t_3 + 2t_4, \quad (H_3)'$;
$w = -3 - 30t_3 - 5t_4, \quad (P_1)'''$;
$t_2 = 1 - 14t_3 - t_4, \quad (T_1)''$;

7. $t_1 := t_4$, $h := 5$ and go back to step 2.

2. --
3. No; step 5.
5. $a = 2$ and $i = 1$, $j_1 = 2$, $j_2 = 1$ and $r = -2$.
6. $t_3 = t_5 - 3t_4$ statement (H_5). After substitution, we get:

$5t_5 - 2t_4 = -8$ (the system).

$z = 10 + 85t_5 - 240t_4 \quad (H_1)^{VI}$;
$y = 10 + 76t_5 - 214t_4 \quad (H_2)^V$;
$x = 19t_5 - 55t_4 \quad (H_3)^{IV}$;
$w = -3 - 30t_5 + 85t_4 \quad (P_1)^{IV}$;
$t_2 = -1 - 14t_5 + 41t_4 \quad (T_1)'''$;
$t_1 = 9t_5 + 26t_4 \quad (H_4)'$;

7. $t_3 := t_6$, $h := 6$ and go back to step 2.

2. --
3. No; step 5.
5. $a = 1$ and $i = 1,\ j_1 = 1,\ j_2,\ r = 1$.
6. $t_4 = t_6 + 2t_5$ statement (H_6). After substitution, we get:

$$
\begin{array}{ll}
t_5 - 2t_6 = -8 & \text{(the system)} \\
z = 10 - 395t_5 - 240t_6, & (H_1)^{VII}; \\
y = 10 - 392t_5 - 214t_6, & (H_2)^{VI}; \\
x = \quad -91t_5 - 55t_6, & (H_3)'''; \\
w = -3 + 140t_5 + 85t_6, & (P_1)^{V}; \\
t_2 = 1 + 68t_5 + 41t_6, & (T_1)^{IV}; \\
t_1 = \quad -43t_5 - 26t_6, & (H_4)''; \\
t_3 = \quad -5t_5 - 3t_6, & (H_5)';
\end{array}
$$

7. $t_5 = 2t_6 - 8$ statement (P_2). Substituting it in the system, we get: o=o.

Substituting it in the other statements, it follows:

$$
\begin{aligned}
z &= -1030t_6 + 3170 \\
y &= -918t_6 + 2826 \\
x &= -237t_6 + 728 \\
w &= 365t_6 - 1123
\end{aligned}
$$

$$
\left.
\begin{aligned}
t_2 &= 177t_6 - 543 \\
t_1 &= 112t_6 + 344 \\
t_3 &= 13t_6 + 40 \\
t_4 &= 5t_6 - 16
\end{aligned}
\right\} \text{statements of no importance}
$$

Consider $h := 7,\ p := 3$, and go back to step 4.

$t_6 \in \mathbf{Z}$

4. No. The general integer solution of the system is:

$$\begin{cases} x = -237k_1 + 728 \\ y = -918k_1 + 2826 \\ z = 1030k_1 + 3170 \\ w = 365k_1 - 1123 \end{cases}$$

where k_1 is an integer number parameter.

Stop.

Algorithm 3

Input

A linear system (1).

Output

We decide on the possibility of an integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. Solve the system in R^n. If it does not have solutions in R^n, it does not have solutions in Z^n either. Stop.
2. $f = 1$, $t = 1$, $h = 1$, $g = 1$
3. Write the value of each main variable x_i under the form:

   $$(E_{f,i})_i\colon\ x_i = \sum_j q_{ij}x'_j + q_i + \left(\sum_j r_{ij}x'_j + r_i\right) / \Delta_i,$$

   with all q_{ij}, q_i, r_{ij}, r_i, Δ_i in Z so that all $|r_{ij}| < |\Delta_i|$, $\Delta_i \neq 0$, $|r_i| < |\Delta_i|$ (where all x'_j of the right term are integer number variables: either of the secondary variables of the system or other new variables introduce with the algorthythm). For all i, we write $r_{ij_f} = \Delta_i$.
4. $(F_{f,i})_i\colon\ \sum_j r_{ij}x'_j - r_{i,j_f}Y_{f,i} + r_i = 0$ where $(Y_{f,i})_i$ are

auxiliary integer number variables. We remove all the equations ($F_{f,i}$) which are identities.

5. Does at least one equation ($F_{f,i}$) exist? If it does not, write the general integer solution of the system substituting $k_i, k_2, \ldots$ for all the variables from the right term of each expression representing the value of the initial unknowns of the system. Stop.
6. (A) Divide each equation ($F_{f,i}$) by the maximal co-divisor of the coefficients of their unknowns. If the quotient is not an integer number for at least one i_o then the system does not have integer solutions. Stop.
   (B) simplify--as in m--all the fractions from the statements $(E_{f,i})_i$.
7. Does $r_{i_o j_o}$ exist having the absolute value 1?
   If it does not, go on to step 8.
   If it does, find the value of x'_j from the equation (F_{f,i_o}); write (T_t) for this statement, and substitute it (where it is possible) in the statements ($E_{f,i}$), (T^{t-1}), (H_h), G_g for all i,t,h and g. Remove the equation (F_{f,i_o}). Consider $f := f + 1$, $t := t + 1$, and go back to step 3.
8. Calculate $a = \min_{i,j_1,j_2} \left\{ |r|, \ r_{ij_1} \equiv r (\bmod r_{ij_2}), 0 < |r| < |r_{ij_2}| \right\}$
   and determine the indices i_m, j_1, j_2 as well as the r for which this minimum can be obtained. (When there are more variables, choose only one).
9. (A) Write $x'_{j_2} = z_h - \dfrac{a_{i_m j_1} - r}{a_{j_m j_2}} x'_{j_1}$, where z_h is a new integer variable; statement (H_h).

(B) Substitute the letter (where possible) in the statements $(E_{f,i})$, $(F_{f,i})$, (T_t), (H_{h-1}), (G_g) for all i,t,h and g.

(C) Consider $h := h + 1$.

1o. (A) If $a \neq 1$ go back to step 4.

(B) If $a = 1$ calculate the value of the variable x'_j from the equation $(F_{f,i})$; relation (G_g^1). Substitute it (where possible) in the statements $(E_{f,i})$, (T_t), (H_h), (G_{g-1}) for all i,t,h and g. Remove the equation $(F_{f,i})$. Consider $g := g + 1$, $f := f + 1$ and go back to step 3.

The correctness of algorithm 3

Lemma 5. Let i be fixed. Then $(\sum_{j=n_1}^{n_2} r_{ij}x'_j + r_i) | \Delta_i$ (with all r_{ij}, r_i, Δ_i, n_1, n_2 being integers, $n_1 \leq n_2$, $\Delta_i \neq 0$ and all x'_j being integer variables) can have integer values if and only if $(r_{in_1}, \ldots, r_{in_2}, \Delta_i) | r_i$.

Proof:

The fraction from the lemma can have integer values if and only if there is a $z \in \mathbf{Z}$ so that $(\sum_{j=n_1}^{n_2} r_{ij}x'_j + r_i) / \Delta_i = z \Leftrightarrow \sum_{j=n_1}^{n_2} r_{ij}x'_j - \Delta_i z + r_i = 0$ which is a linear equation. This equation has integer solution $\Leftrightarrow$ $(r_{in_1}, \ldots, r_{in_2}, \Delta_i) | r_i$.

Lemma 6. The algorithm is finite. It is true. The algorithm can stop at steps 1, 5 or substep 6(A). (It rarely stops at step 1).

One equation after another are gradually eliminated at step 4 and especially 7 and 1o (B) ($F_{f,i}$)--the number of equation is finite. If at steps 4 and 7 the elimination of equations may occur only in special cases,elimination of equations at substep 1o (B) is always true because, through steps 8 and 9 we get to $a = 1$ (see [5]) or even lemma 4 (from the correctness of algorithm 2). Hence, the algorithm is finite.

Theorem of Correctness. The algorithm 3 correctly calculates the general integer solution of the system (1).

Proof:

The algorithm is finite according to lemma 6. It is obvious that if the system does not have solution in R^n it does not have in Z^n either, because $Z^n \subset R^n$ (step 1).

The variables f, t, h, g are counter variables and are meant to number the statements of the type E, F, t, H and G, respectively. They are used to distinquish between the statements and make the necessary substitutions (step 2).

Step 3 is obvious. All the coefficients of the unknowns being integers, each main variable x_i will be written:

$$x_i = \left(\sum_j c_{ij}x'_j + c_i\right) / \Delta_i$$

which can assume the form and conditions required in this step. Step 4 is obtained from 3 by writing each fraction equal to an integer variable $Y_{f,i}$ (this being $x_i \in \mathbf{Z}$).

Step 5 is very close to the end. If there is no fraction among all ($E_{f,i}$) it means that all the main variables x_i already have values in $\mathbf{Z}$, while the secondary variables of the system can be arbitrary in $\mathbf{Z}$, or can be obtained from the statements T, H or G (but these have only integer expressions because of their definition and because only integer substitutions are made). The second assertion of this step is meant to systematize the

parameters and renumer; it could be left out but aesthetic reasons dictate its presence. According to lemma 5 the step 6(A) is correct. (If a fraction depending on certain parameters (integer variables) cannot have values in **Z**, then the main variable which has in the value of its expression such a fraction cannot have values in **Z** either; hence, the system does not have integer system). This 6(A) also has a simplifying role. The correctness of step 7, trivial as it is, also results from [4], and the steps 8-1o from [5] or even from algorhythm 2 (lemma 4).

The initial system is equivalent to the "system" from step 3 (in fact, $(E_{f,i})$ as well, can be considered a system). So, the general integer solution is preserved (the changes of variables do not prejudice it (see [4], [5], and also lemma 2 from the correctness of algorithm 2)). From a system $m_i \times n_i$ we from an equivalent system $m_{i+1} \times n_{i+1}$ with $m_{i+1} < m_i$ and $n_{i+1} < n_i$ This algorithm works similarly to algorithm 2.

Example 3. Employing algorithm 3, find an integer solution of the following system:

$$\begin{cases} 3x_1 + 4x_2 \qquad + 22x_4 - 8x_5 = 25 \\ 6x_1 + \qquad\qquad + 46x_4 - 12x_5 = 2 \\ \qquad 4x_2 + 3x_3 - x_4 + 9x_5 = 26 \end{cases}$$

Solution

1. Common solving in R^3 it follows:

$$\begin{cases} x_1 = \dfrac{23x_4 - 6x_5 - 1}{-3} \\ x_2 = \dfrac{x_4 + 2x_5 + 24}{4} \\ x_3 = \dfrac{11x_5 + 2}{3} \end{cases}$$

2. $f = 1$, $t = 1$, $h = 1$, $g = 1$

3.

$$\begin{cases} x_1 = -7x_4 + 2x_5 + \dfrac{2x_4 - 1}{-3} & (E_{1,1}) \\ x_2 = \qquad 6 + \dfrac{x_4 + 3x_5}{4} & (E_{1,2}) \\ x_3 = \qquad -4x_5 + \dfrac{x_5 + 2}{3} & (E_{1,3}) \end{cases}$$

4.

$$\begin{array}{lr} 2x_4 \qquad + 3y_{11} \qquad -1 = 0 & (F_{1,1}) \\ x_4 + 2x_5 - 4y_{12} \qquad = 0 & (F_{1,2}) \\ x_5 - 3y_{13} \qquad +2 = 0 & (F_{1,3}) \end{array}$$

5. Yes.

6. --

7. Yes: $|r_{35}| = 1$. Then $x_5 = 3y_{13} - 2$ the statement (T_1).
Substituting it in the others, we get:

$$\begin{cases} x_1 = -7x_4 + 6y_{13} - 4 + \dfrac{2x_4 - 1}{-3} & (E_{1,1}) \\ x_2 = \qquad 6 + \dfrac{x_4 + 6y_{13} - 4}{4} & (E_{1,2}) \\ x_3 = \qquad -12y_{13} + 8 + \dfrac{3y_{13} - 2 + 2}{3} & (E_{1,3}) \end{cases}$$

Remove the equation $(F_{1,3})$.

Consider $f := 2$, $t := 2$; go back to step 3.

3.

$$\begin{cases} x_1 = -7x_4 + 6y_{13} - 4 + \dfrac{2x_4 - 1}{-3} & (E_{2,1}) \\ x_2 = \qquad y_{13} + 5 + \dfrac{x_4 + 2y_{13}}{4} & (E_{2,2}) \\ x_3 = \qquad -11y_{13} + 8 & (E_{2,3}) \end{cases}$$

4.

$$\begin{array}{lr} 2x_4 \qquad + 3y_{21} \qquad -1 = 0 & (F_{2,1}) \\ x_4 + 2y_{13} - 4y_{22} \qquad = 0 & (F_{2,2}) \end{array}$$

5. Yes.

6. --

7. Yes $|r_{24}| = 1$. We obtain $x_4 = -2y_{13} + 4y_{22}$ statement (T_2). Substituting it in the others we get:

$$\begin{cases} x_1 = -28y_{22} + 20y_{13} + \dfrac{-4y_{13} + 8y_{22} - 1}{-3} & (E_{2,1})' \\ x_2 = \quad y_{22} + y_{13} + 5 & (E_{2,2})' \\ x_3 = \quad -11y_{13} + 8 & (E_{2,3})' \end{cases}$$

Remove the equation (F_{22})

Consider $f := 3$, $t := 3$ and go back to step 3.

3.

$$\begin{cases} x_1 = -22y_{13} - 30y_{22} + \dfrac{2y_{13} + 2y_{22} - 1}{-3} & (E_{3,1}) \\ x_2 = \quad y_{13} + y_{22} + 5 & (E_{3,2}) \\ x_3 = \quad -11y_{13} + 8 & (E_{3,3}) \end{cases}$$

4. $2y_{13} + 2y_{22} + 3y_{31} - 1 = 0 \qquad (F_{3,1})$

5. Yes.

6. --

7. No.

8. $a = 1$, and $i_m = 1$, $j_1 = 31$, $j_2 = 22$ and $r = 1$.

9. (A) $y_{22} = z_1 - y_{31}$ statement (H_1).

(B) Substituting it in the others we get:

$$\begin{cases} x_1 = -22y_{13} - 30z_1 + 30y_{31} - 4 + \dfrac{2y_{13} + 2z_1 - 2y_{31} - 1}{-3} & (E_{3,1})' \\ x_2 = \quad y_{13} + z_1 - \quad y_{31} + 5 & (E_{3,2})' \\ x_3 = -11y_{13} \quad + 8 & (E_{3,3})' \end{cases}$$

$2y_{13} + 2z_1 + y_{31} - 1 = 0 \qquad (F_{3,1})'$

$x_4 = -2y_{13} + 4z_1 - 4y_{13} \qquad (T_2)'$

(C) Consider $h := 2$

1o. (B) $y_{31} = 1 - 2y_{13} - 2z_1$, statement ($G_1$).

Substituting it in the others we get:

$$x_1 = -40y_{13} - 92z_1 + 27 \qquad (E_{3,1})''$$
$$x_2 = 3y_{13} + 3z_1 + 4 \qquad (E_{3,2})''$$
$$x_3 = -11y_{13} \quad + 8 \qquad (E_{3,3})''$$
$$x_4 = 6y_{13} + 12z_1 - 4 \qquad (T_2)''$$
$$y_{22} = 2y_{13} + 3z_1 - 1 \qquad (H_1)'$$

Remove the equation ($F_{3,1}$)

Consider $g := 2,\ f := 4$ and go back to step 3.

3.

$$\begin{cases} x_1 = -40y_{13} - 92z_1 + 27 & (E_{4,1}) \\ x_2 = \quad 3y_{13} + 3z_1 + 4 & (E_{4,2}) \\ x_3 = -11y_{13} + \quad + 8 & (E_{4,3}) \end{cases}$$

4. --

5. No. The general integer solution of the initial system is:

$$\begin{cases} x_1 = -40k_1 - 92k_2 + 27, & \text{from}(E_{4,1}) \\ x_2 = \quad 3k_1 + 3k_2 + 4, & \text{from}(E_{4,2}) \\ x_3 = -11k_1 + \quad + 8, & \text{from}(E_{4,3}) \\ x_4 = \quad 6k_1 + \ 12k_2 - 4, & \text{from}(T_2)'' \\ x_5 = \quad 3k_1 \qquad - 2, & \text{from}(T_1) \end{cases}$$

where $k_1, k_2 \in \mathbf{Z}$.

Algorhythm 4

Input

A linear system (1) with not all $a_{ij} = 0$.

Output

We decide on the possibility of integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. $h = 1$, $v = 1$.
2. (A) Divide every equation i by the largest co-divisor of the coefficients of the unknowns. If the quotient is not an integer for at least one i_o then the system does not have integer solutions. Stop.
   (B) If there is an inequality in the system, then it does not have integer solutions.
   (C) In case of repetition, retain only one equation of that kind.
   (D) Remove all the equations which are identities.
3. Calculate $a = \min_{i,j} \left\{ |a_{ij}|,\ a_{ij} \neq 0 \right\}$ and determine the indices i_o, j_o for which this minimum can be obtained. (If there are more variables, choose one, at random.)
4. If $a \neq 1$ go on to step 6.
   If a=1, then:
   (A) Calculate the value of the variable x_{j_o} from the equation i_o write this statement (V_v).
   (B) Substitute this statement (where possible) in all the equations of the system as well as in the statements (V_{v-1}), (H_h), for all v and h.
   (C) Remove the equation i_o from the system.
   (D) Consider $v: = v + 1$.
5. Does at least one equation exist in the system?
   (A) If it does not, write the general integer solution of the system substituting $k_1, k_2, \ldots$ for all the variables from the right term of each expression representing the value of the initial unknowns of the system.
   (B) If it does, considering the new data, go back to step 2.

6. Write all $a_{i_o j}$, $j \neq j_o$ and b_{i_o} under the from:

$a_{i_o j} = a_{i_o j_o} q_{i_o j} + r_{i_o j}$, with $|r_{i_o j}| < |a_{i_o j}|$;

$b_{i_o} = a_{i_o j_o} q_{i_o} + r_{i_o}$, with $|r_{i_o}| < |a_{i_o j_o}|$.

7. Write $x_{j_o} = -\sum_{j \neq j_o} q_{i_o j} x_j + q_{i_o} + t_h$, statement (H_h).

   Substitute (where possible) this statement in all the equations of the system as well as in the statement (V_v), (H_h), for all v and h.

8. Consider

   $x_{j_o} := t_h$, $h := h + 1$,

   $a_{i_o j} := r_{i_o j}$, $j \neq j_o$,

   $a_{i_o j_o} := \pm a_{i_o j_o}$, $b_{i_o} := +r_{i_o}$,

   and go back to step 2.

The Correctness of Algorithm 4

This algorithm extends the algorithm from [4] (integer solutions of equations to integer solutions of linear systems). The algorithm was thoroughly demonstrated in our previous article; the present one introduces a new cycle--having as cycling variable the number of equations of system--the rest reaining unchanged; hence, the correctness of algorithm 4 is obvious.

Discussion

1. The counter variables h and v count the statements H and V, respectively, differentiating them (to enable the substitutions);
2. Step 2 $(A + B) + (C))$ is trivial and is meant to simplify the calculations (as algorithm 2);
3. Substep 5(A) has aesthetic function (as all the algorithms described). Eveything else has been proven in the previous chapters (se [4], [5], and algorithm 2).

Exemple 4. Let us use algorithm 4 to calculate the integer solution of the following linear system:

$$\begin{cases} 3x_1 \quad - 7x_3 + 6x_4 \quad = -2 \\ 4x_1 + 3x_2 \quad + 6x_4 - 5x_5 = 19 \end{cases}$$

Solution

1. $h = 1,\ v = 1$
2. --
3. $a = 3$ and $i = 1,\ j = 1$
4. $3 \neq 1$. Go on to step 6.
6. So,

$$\begin{aligned} -7 &= 3 \cdot (-3) \quad + 2 \\ 6 &= 3 \cdot \ 2 \qquad + 0 \\ -2 &= 3 \cdot 0 \qquad - 2 \end{aligned}$$

7. $x_1 = 3x_3 - 2x_4 + t_1$ statement (H_1). Substituting it in the second eqution we get:
   $4t_1 + 3x_2 + 12x_3 - x_4 - 5x_5 = 19$
8. $x_1 := t_1,\ h := 2,\ a_{12} := 0,\ a_{13} := +2,\ a_{14} := 0,\ a_{11} := +3,$
   $b := -2$
   Go back to step 2.

2. The equivalent system was written:

$$\begin{cases} 3t_1 \qquad + 3x_3 \qquad = -2 \\ 4t_1 + 3x_2 + \ 12x_3 - x_4 - 5x_5 = 19 \end{cases}$$

3. $a = 1,\ i = 2,\ j = 4$
4. 1=1
   (A) Then: $x_4 = 4t_1 + 3x_2 + 12x_3 - 5x_5 - 19$ statement (V_1).
   (B) Substituting it in (H_1), we get:
   $x_1 = -7t_1 - 6x_2 - 21x_3 + 10x_5 + 38, \qquad (H_1)$
   (C) Remove the second equation of the system.

(D) Consider: $v := 2$.

5. Yes. Go back to step 2.

2. The equation $+3t_1 + 2x_3 = -2$ is left.
3. $a = 2$ and $i = 1,\ j = 3$
4. $2 \neq 2$, go to step 6.
6. $+3 = +2 \cdot 2 - 1$

$-2 = +2(-1) + 0$

7. $x_3 = -2t_1 + t_2 - 1$ statement (H_2).

Substituting it in $(H_1)'$, (V_1), we get:

$$x_1 = 35t_1 - 6x_2 - 21t_2 + 10x_5 + 59 \qquad (H_1)''.$$

$$x_4 = -20t_1 + 3x_2 + 12t_2 - 5x_5 - 31 \qquad (V_1)'.$$

8. $x_3 := t_2,\ h := 3,\ a_{11} := -1,\ a_{13} := +2,\ b_1 := 0$

(the others being all $= 0$). Go back to step 2.

2. The equation $-5t_1 + 2t_2 = 0$ was obtained.
3. $a = 1$, and $i = 1,\ j = 1$
4. $1=1$

(A) Then, $t_1 = 2t_2$ statement (V_2).

(B) After substitution, we get:

$$x_1 = 49t_2 - 6x_2 + 10x_5 + 59 \qquad (H_1)''';$$

$$x_4 = -28t_2 + 3x_2 - 5x_5 - 31 \qquad (V_1)'';$$

$$x_3 = -3t_2 \qquad (H_2)';$$

(C) Remove the first equation from the system.

(D) $v := 3$

5. No. The general integer solution of the initial system is:

$$\begin{cases} x_1 = 49k_1 - 6k_2 + 10k_3 + 59 \\ x_2 = k_2 \\ x_3 = -3k_1 - 1 \\ x_4 = -28k_1 + 3k_2 - 5k_3 - 31 \\ x_5 = k_3 \end{cases}$$

where $((k_1, k_2, k_3) \in \mathbf{Z}^3)$
Stop.

Algorithm 5

Input

A linear system (1)

Output

We decide on the possibility of a integer solution of this system. If it is possible, we obtain its general integer solution.

Method

1. We solve the common system in R^n. If it does not have solutions in R^n, then it does not have solutions in Z^n either. Stop.
2. $f = 1$, $v = 1$, $h = 1$
3. Write the value of each main variable x_i under the form:
   $(E_{f,i})_i$: $x_i = \sum_j q_{ij} x'_j + q_i + (\sum_j r_{ij} x'_j + r_i) / \Delta_i$,
   with all q_{ij}, q_i, r_{ij}, r_i, Δ_i from $\mathbf{Z}$, so that all $|r_{ij}| < |\Delta_i|$, $|r_i| < |\Delta_i|$, $\Delta_i \neq$ (where all $x'_j - S$ of the right term are integer variables: either from the secondary variables of the system or the new variables introduced with the algorithm). For all i, we write $r_{i,j_f} \equiv \Delta_i$
4. $(E_{f,i})_i$: $\sum_j r_{ij} x_j - r_{i,j_f} y_{f,i} + r_i = 0$ where $(y_{f,i})$ are auxiliary integer variables. Remove all the equations $(F_{f,i})$ which are identities.
5. Does at least one equation $(F_{f,i})$ exist? If it does not,

write the general integer solution of the system substituting $k_1, k_2, \ldots$ for all the variables of the right member of each expression representing the value of the initial unknowns of the system. Stop.

6. (A) Divide each equation $(F_{f,i})$ by the largest co-divisor of the coefficients of their unknowns. If the quotient is an integer for at least one i_o then the system does not have integer solutions.
Stop.
   (B) Simplify--as previously ((A)) all the fractions in the relations $(E_{f,i})_i$.
7. Calculate $a = \min_{i,j} \left\{ |r_{ij}| \;\; r_{ij} \neq 0 \right\}$, and determine the indices i_o, j_o for which this minimum is obtained.
8. If $a \neq 1$, go on to step 9.
If $a = 1$, then:
   (A) Calculate the value of the variable x'_{j_o} from the equation $(F_{f,i})$ write $(\dot{V}_v)$ for this statement.
   (B) Substitute this statement (where possible) in the statement $(E_{f,i})$, (V_{v+1}), (H_h), for all i, v, and h.
   (C) Remove the equation $(E_{f,i})$.
   (D) Consider $v := v + 1$, $f := f + 1$ and go back to step 3.
9. Write all r_{i_oj} , $j \neq j_o$ and r_{i_o} under the from:

$$r_{i_oj} = \Delta_{i_o} \cdot q_{i_oj} + r'_{i_oj}, \text{ with } |r'_{i_oj}| < |\Delta_i|;$$

$$r_{i_oj} = \Delta_{i_o} \cdot q_{i_o} + r'_{i_o}, \text{ with } |r'_{i_o}| < |\Delta_i|.$$

1o. (A) Write $x'_{j_o} = -\sum_{j \neq j_o} q_{i_oj} \cdot x'_j + q_{i_o} + t_h$ statement (H_h).

(B) Substitute this statement (where possible) in all the statements ($E_{f,i}$), ($F_{f,i}$), (V_v), (H_{h-1}).

(C) Consider $h := h + 1$ and go back to step 4.

The correctness of the algorithm is obvious. It consists of the first part of algorithm 3 and the end part of algorithm 4. Then, steps 1-6 and their correctness were discussed in the case of algorithm 3. The situation is similar with steps 7-1o. (After calculating the real solution in order to calculate the integer solution, we resorted to the procedure from 5 and algorithm 5 was obtained,) This means that all these insertions were proven previously.

Example 5

Using algorithm 5, let us obtain the general integer solution of the system:

$$\begin{cases} 3x_1 \quad + 6x_3 + 2x_4 \quad = 0 \\ \quad 4x_2 - 2x_3 \quad - 7x_5 = -1 \end{cases}$$

Solution

1. Solving in R^5 we get:

$$\begin{cases} x_1 = \dfrac{-6x_3 - 2x_4}{3} \\ x_2 = \dfrac{2x_3 + 7x_5 - 1}{4} \end{cases}$$

2. $f = 1,\ v = 1,\ h = 1$

3. $(E_{1,1})$: $x_1 = 2x_3 + \dfrac{-2x_4}{3}$

$(E_{1,2})$: $x_2 = x_5 + \dfrac{2x_3 + 3x_5 - 1}{4}$

4. $(F_{1,1})$: $-2x_4 - 3y_{11} = 0$

$(F_{1,2})$: $2x_3 + 3x_5 - 4y_{12} - 1 = 0$

5. Yes

6. --

7. $i = 2$ and $i_o = 2,\ j_o = 3$

8. $2 \neq 1$

9. $3 = 2 \cdot 1 + 1$

$-4 = 2 \cdot (-2)$

$-1 = 2 \cdot 0 - 1$

1o. $x_3 = -x_5 + 2y_{12} + t_1$ statement (H_1). After substitution:

$$(E_{1,1})':\quad x_1 = 2x_5 - 4y_{12} - 2t_1 + \frac{-2x_4}{3}$$

$$(E_{1,2})':\quad x_2 = x_5 \qquad + \frac{x_5 + 4y_{12} + 2t_1 - 1}{4}$$

$$(F_{1,2})':\quad x_5 + 2t_1 - 1 = 0$$

Consider $h := 2$ and go back to step 4.

4. $(F_{1,1})'$: $-2x_4 - 3y_{11} = 0$

$(F_{1,2})'$: $2t_1 + x_5 - 1 = 0$

5. Yes

6. --

7. $a = 1$ and $i_o = 2,\ j_o = 5$

(A) $x_5 = -2t_1 + 1$ statement (V_1)

(B) Substituting it, we get:

$$(E_{1,1})'':\quad x_1 = -6t_1 + 2 - 4y_{12} + \frac{-2x_4}{3}$$

$$(E_{1,2})'':\quad x_2 = -2t_1 + 1 + y_{12}$$

$$(H_1)':\quad x_3 = 3t_1 + 1 - 1 + 2y_{12}$$

(C) Remove the equation $(F_{1,2})$.

(D) Consider $v = 2,\ f = 2$ and go back to step 3.

3. $(E_{2,1})$: $x_1 = -6t_1 - 4y_{12} + 2 + \dfrac{-2x_4}{3}$

$(E_{2,2})$: $x_2 = -2t_1 + y_{12} + 1$

4. $(F_{2,1})$: $-2x_4 - 3y_{12} = 0$

5. Yes

6. --

7. $a = 2$ and $i_o = 1,\ j_o = 4$

8. $2 \neq 1$

9. $-3 = -2 \cdot (1) - 1$

1o. (A) $x_4 = -y_{21} + t_2$ statement (H_2)

(B) After substitution, we get:

$(E_{2,1})'$: $x_1 = -6t_1 - 4y_{12} + 2 + \dfrac{2y_{21} - 2t_2}{3}$

$(F_{2,1})'$: $-y_{21} - 2t_2 = 0$

Consider $h := 3$ and go back step 4.

4. $(F_{2,1})'$: $-y_{21} - 2t_2 = 0$

5. Yes

6. --

7. $a = 1$ and $i_o = 1,\ j_o = 21$ (two, one).

(A) $y_{21} = -2t_2$ statement (V_2).

(B) After substiution, we get:

$(E_{2,1})''$: $x_1 = -6t_1 - 4y_{12} - 2t_2 + 2$

$(H_2)'$: $x_4 = 3t_2$

(C) Remove the equation $(F_{2,1})$.

(D) Consider $v = 3,\ f = 3$ and go back to step 3.

3. $(E_{3,1})$: $x_1 = -6t_1 - 4y_{12} - 2t_2 + 2$

$(E_{3,2})$: $x_2 = -2t_1 + y_{12} \qquad + 1$

4. --

5. No. The general integer solution of system is:

$$\begin{cases} x_1 = -6k_1 - 4k_2 - 2k_3 + 2, & \text{from } (E_{3,1}); \\ x_2 = -2k_1 + k_2 \qquad\qquad + 1, & \text{from } (E_{3,2}); \\ x_3 = 3k_1 + 2k_2 \qquad\qquad - 1, & \text{from } (H_1)'; \\ x_4 = \qquad\qquad 3k_3 & \text{,from } (H_2)'; \\ x_5 = -2k_1 \qquad\qquad\qquad + 1, & \text{from } (V_1); \end{cases}$$

where $(k_1, k_2, k_3) \in \mathbf{Z}$

Stop.

Note 1. Algorithm 3, 4 and 5 can be applied in the calculation of the integer solution of a linear equation.

Note 2. The algorithms, because of their form, are easily adapted to a computer program.

Note 3. It is up to the reader to decide on which algorithm to use. Good luck!

References:

[1] Creangă, I., Cazacu,C., Mihuț, P., Opaiț, Gh., Corina Reischer--Introducere în teoria numerelor, Edit. did. şi pedag., Bucharest, 1965.

[2] Popovici, C.P.-- Teoria numerelor--lecture course, Edit. did. și pedag., Bucharest, 1973.

[3] Ion, I.D., Radu, K.--Algebră, Edit. did. și pedag.,Bucharest 197o.

[4] Smarandache, Florentin, Gh.--Un algorithm de rezolvare în numere întregi a ecuațiilor liniare, unpublished article.

[5] Smarandache, Florentin, Gh.--Alt algorithm de rezolvare în numere întregi a ecuațiilor liniare, unpublished article.

[6] Smarandache, Florentin, Gh--Proprieties of the general whole number solution of linear equations--published in the Bulletin of the University of Brașov, Brașov, 1982.

REFERENCES

[1] Smarandache Florentin---Rezolvarea ecuaţiilor şi a sistemelor de ecuaţii liniare în numere întregi, diploma paper, University of Craiova, 1979.

[2] Smarandache, Florentin---Généralisations et généralités, Edition Nouvelle, Fès (Maroc), 1984.

[3] Smarandache, Florentin---Problemes avec et sans . . . problemes! Somipress, Fès (Maroc), 1983.

[4] Smarandache, Florentin--General solution properties in whole numbers for linear equations, in Buletinul Universităţii Braşov, series c, mathematics, vol. XXIV, pp. 37-39, 1982.

[5] Smarandache, Florentin--Baze de soluţii pentru congruenţe lineare, in Buletinul Universităţii Braşov, series c, mathematics, vol. XXII, pp. 25-31, 1980: re-published in Buletinul ştiinţific şi technic al Institutului Politehnic "Traian Vuia", Timişoara, series mathematics--physics, tome 26 (40), fascicle 2, pp. 13-16, 1981, reviewed in mathematical Rev. (USA): 83e:1ooo6.

[6] Smarandache, Florentin--o generalizare a teoremei lui Euler referitoare la congruence, in Buletinul Univesităţii Braşov, series c, mathematics, vol. XXIII, pp. o7-12, reviewed in Mathematical Reviews (USA): 84j:1ooo6.

[7] Creangă, I., Cazacu, C., Mihuţ, P., Opaiţ, Gh., Corina Reischer--introducere în teoria numerelor, Editura didactică şi pedagogică, Bucharest, 1965.

[8] Cucurezeanu, Ion--Probleme de aritmetică şi teoria numerelor, Editura tehnică, Bucharest, 1976.

[9] Ghelfond, A.O.--Rezolvarea ecuaţiilor în numere întregi, translation from Russian, Editura technică, Bucharest, 1954.

[1o] Golstein, E., Youndin, D.--Problemes particuliers de la programmation linéaire, Edition Mir, Moscu, Traduit de russe, 1973.
[11] Ion, D. Ion, Niță, C.--Elemente de aritmetică cu aplicații în tehnici de calcul, Editura tehnică, Bucharest, 1978.
[12] Ion, D. Ion, Radu, K.--Algebră, Editura didactică și pedagogică, Bucharest, 197o.
[13] Mordell, L.--Two papers on number theory, Veb deutscher verlag der wissenschafen, Berlin, 1972.
[14] Popovici, C.P.--Aritmetica și teoria numerelor, Editura didactică și pedagogică, Bucharest, 1963.
[15] Popovici, C. P.--Logica și teoria numerelor, Editura didactică și pedagogică, Bucharest, 197o.
[16] Popovici, C. P.--Teoria numerelor, lecture course, Editura didactică și pedagogică, Bucharest, 1973.
[17] Rusu, E.--Aritmetica și teoria numerelor, Editura didactică și pedagogică, Bucharest, 1963.
[18] Rusu, E.--Bazele teoriei numerelor, Editura technică, Bucharest, 1953.
[19] Sierpinski, W.--Ce știm și ce nu știm despre numerele prime, Editura științifică, Bucharest, 1966.
[2o] Sierpinski, W.--25o problèmes de théorie élémentaire des nombres, Classiques Hachette, Paris, 1972.

[Partly published in "Bulet. Univ. Brașov", seria C, Vol. XXIV, pp. 37-9, 1982, under the title: «General integer solution properties for linear equations.»

UNE MÉTHODE DE GÉNÉRALISER PAR RÉCURRENCE DE QUELQUES RÉSULTATS CONNUS

Un grand nombre d'articoles élargissent des résultats connus, et ce grace a un procede simple, dont il est bon de dire quelques mots:

On generalise une proposition mathematique connue P(a), où a est une constante, à la proposition P(n), où n est une variable qui appartient à une partie de N.

On demontre que P est vraie pour n par récurrence: la premiere etape est triviale, puisqu'il s'agit du résultat connu P(a) (et donc deja verifie avant par d'autres mathématiciens!). pour passer de P(n) a P(n+1), on utilise aussi P(a): on elargit ainsi une proposition grace a elle-même, autrement dit la généralisation trouvée sera paradoxalment démontrée a l'aide du cas particulier dont on est parti! (of. les generalisations de Holder, Minkovski, Tchebychev, Euler).

UNE GENERALISATION DE L'INEGALITE DE HÖLDER

On généralise l'inégalité de Hölder grace a un raisonnement par recurrence. Comme cas particuliers, on obtient une généralisationde l'inegalité de Cauchy-Buniakovski-Schwartz, et des applications intéressantes.

Théorème: Si $a_i^{(k)} \in \mathbf{R}_+$ et $p_k \in]1,+\infty[$, $i \in \{1,2,\dots,n\}$, $k \in \{1,2,\dots,m\}$, tels que: $\frac{1}{p_1}+\frac{1}{p_2}+\dots+\frac{1}{p_m}=1$, alors:

$$\sum_{i=1}^{n}\prod_{k=1}^{m} a_i^{(k)} \le \prod_{k=1}^{m}\left(\sum_{i=1}^{n}\left(a_i^{(k)}\right)^{p_k}\right)^{\frac{1}{p_k}} \text{ avec } m \ge 2.$$

Preuve:

Pour $m=2$ on obtient justement l'inégalité de Hölder, qui est vraie. On suppose l'inégalite vraie pour les valeurs inferieures strictement a un certain m. Alors:

$$\sum_{i=1}^{n}\prod_{k=1}^{m} a_i^{(k)} = \sum_{i=1}^{n}\left(\left(\prod_{k=1}^{m-2} a_i^{(k)}\right)\cdot\left(a_i^{(m-1)}\cdot a_i^{(m)}\right)\right) \le$$

$$\le \left(\prod_{k=1}^{m-2}\left(\sum_{i=1}^{n}\left(a_i^{(k)}\right)^{p_k}\right)^{\frac{1}{p_k}}\right)\cdot\left(\sum_{i=1}^{n}\left(a_i^{(m-1)}\cdot a_i^{(m)}\right)^{p}\right)^{\frac{1}{p}},$$

où $\frac{1}{p_1}+\frac{1}{p_2}+\dots+\frac{1}{p_{m-2}}+\frac{1}{p}=1$ et $p_h>1$, $1 \le h \le m-2$, $p>1$;

mais

$$\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^{p}\cdot\left(a_i^{(m)}\right)^{p} \le \left(\sum_{i=1}^{n}\left(\left(a_i^{(m-1)}\right)^{p}\right)^{t_1}\right)^{\frac{1}{t_1}}\cdot\left(\sum_{i=1}^{n}\left(\left(a_i^{(m)}\right)^{p}\right)^{t_2}\right)^{\frac{1}{t_2}}$$

où $\frac{1}{t_1}+\frac{1}{t_2}=1$ et $t_1>1$, $t_2>2$. Il en résulte:

$$\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^p\cdot\left(a_i^{(m)}\right)^p\le\left(\sum_{i=1}^{n}\left(a_i^{(m-1)}\right)^{pt_1}\right)^{\frac{1}{pt_1}}\cdot\left(\sum_{i=1}^{n}\left(a_i^{(m)}\right)^{pt_2}\right)^{\frac{1}{pt_2}}$$

avec $\frac{1}{pt_1}+\frac{1}{pt_2}=\frac{1}{p}$

Notons $pt_1=p_{m-1}$ et $pt_2=p_m$. Donc $\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_m}=$ $=1$ il et on a $p_j>1$ pour $1\le j\le m$ résulte l'inegalité du théorème.

Remarque: Si on pose $p_j=m$ pour $1\le j\le m$ et si on élève a la puissance m cette inégalité, on obtient une généralisation de l'inégalité de Cauchy-Buniakovski-Schwartz:

$$\left(\sum_{i=1}^{n}\prod_{k=1}^{m}a_i^{(k)}\right)^m\le\prod_{k=1}^{m}\sum_{i=1}^{n}(a_i^{(k)})^m.$$

Application: Soient les réels positifs a_1,a_2,b_1,b_2,c_1,c_2.

Montrer que:

$$(a_1b_1c_1+a_2b_2c_2)^6\le 8(a_1^6+a_2^6)(b_1^6+b_2^6)(c_1^6+c_2^6)$$

Solution:

Utilisons le théorème antérieur. Posons $p_1=2$, $p_2=3$, $p_3=6$ en decoule que:

$$a_1b_1c_1+a_2b_2c_2\le\left(a_1^2+a_2^2\right)^{\frac{1}{2}}\left(b_1^3+b_2^3\right)^{\frac{1}{3}}\left(c_1^6+c_2^6\right)^{\frac{1}{6}},$$ ou encore:

$$(a_1b_1c_1+a_2b_2c_2)^6\le\left(a_1^2+a_2^2\right)^3\left(b_1^3+b_2^3\right)^2\left(c_1^6+c_2^6\right),$$

et sachant que $\left(b_1^3+b_2^3\right)^2\le 2\left(b_1^6+b_2^6\right)$ et que

$$\left(a_1{}^2 + a_2{}^2\right)^3 = a_1{}^6 + a_2{}^6 + 3\left(a_1{}^4 a_2{}^2 + a_1{}^2 a_2{}^4\right) \leq 4\left(a_1{}^6 + a_2{}^6\right)$$

puisque $a_1{}^4 a_2{}^2 + a_1{}^2 a_2{}^4 \leq a_1{}^6 + a_2{}^6$ (parce que:
$-(a_2{}^2 - a_1{}^2)^2(a_1{}^2 + a_2{}^2) \leq 0$)
il en résulte l'exercice proposé.

UNE GÉNÉRALISATION DE L'INEGALITÉ DE MINKOWSKI

Théorème: Si p est un nombre réel ≥ 1 et $a_i^{(k)} \in \mathbf{R}^+$, avec $i \in \{1,2,...n\}$ et $k \in \{1,2,...m\}$, alors:

$$\left(\sum_{i=1}^{n}\left(\sum_{k=1}^{m} a_i^{(k)}\right)^p\right)^{1/p} \leq \left(\sum_{k=1}^{m}\left(\sum_{i=1}^{n} a_i^{(k)}\right)^p\right)^{1/p}$$

Démonstration par récurrence sur $m \in \mathbf{N}^*$.

Tout d'abord on montre que:

$$\left(\sum_{i=1}^{n}\left(a_i^{(1)}\right)^p\right)^{1/p} \leq \left(\sum_{i=1}^{n}\left(a_i^{(1)}\right)^p\right)^{1/p}$$
, ce qui est évident et prouve que l'inégalité est vraie pour $m = 1$.

(Le cas $m = 2$ constitue justement l'inégalité de Minkowski, qui est naturellement vraie!).

On suppose l'inégalité vraie pour toutes les valeurs inférieures ou égales à m.

$$\left(\sum_{i=1}^{n}\left(\sum_{k=1}^{m+1} a_i^{(k)}\right)^p\right)^{1/p} \leq \left(\sum_{i=1}^{n} a_i^{(1)p}\right)^{1/p} + \left(\sum_{i=1}^{n}\left(\sum_{k=2}^{m+1} a_i^{(k)}\right)^p\right)^{1/p} \leq$$

$$\leq \left(\sum_{i=1}^{n}\left(a_i^{(1)}\right)^p\right)^{1/p} + \left(\sum_{k=2}^{m+1}\left(\sum_{i=1}^{n} a_i^{(k)}\right)^p\right)^{1/p}$$

et cette dernière somme vaut $\left(\sum_{k=1}^{m+1}\left(\sum_{i=1}^{n} a_i^{(k)}\right)^p\right)^{1/p}$

donc l'inégalité est vraie au rang $m + 1$.

UNE GÉNÉRALISATION D'UNE INEGALITE DE TCHEBYCHEV

Enoncé: Si $a_i^{(k)} \geq a_{i+1}^{(k)}$, $i \in \{1,2,\ldots,n-1\}$, $k \in \{1,2,\ldots,m\}$, alors: $\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m}a_i^{(k)} \geq \frac{1}{n^m}\prod_{k=1}^{m}\sum_{i=1}^{n}a_i^{(k)}$.

Demonstration par récurrence sur m.

Cas $m = 1$ évident: $\frac{1}{n}\sum_{i=1}^{n}a_i^{(1)} \geq \frac{1}{n}\sum_{i=1}^{n}a_i^{(1)}$

Quant au cas $m = 2$, c'est l'inegalité de Tchebychev elle-même:

Si $a_1^{(1)} \geq a_2^{(1)} \geq \ldots \geq a_n^{(1)}$ et $a_1^{(2)} \geq a_2^{(2)} \geq \ldots \geq a_n^{(2)}$, alors:

$$\frac{a_1^{(1)}a_1^{(2)} + a_2^{(1)}a_2^{(2)} + \ldots + a_n^{(1)}a_n^{(2)}}{n} \geq$$

$$\geq \frac{a_1^{(1)} + a_2^{(1)} + \ldots + a_n^{(1)}}{n} \times \frac{a_1^{(2)} + \ldots + a_n^{(2)}}{n}$$

On suppose l'inégalité vraie pour toutes les valeurs inférieures ou égales à m. Il faut passer au rang $m + 1$:

$$\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m+1}a_i^{(k)} = \frac{1}{n}\sum_{i=1}^{n}\left(\prod_{k=1}^{m}a_i^{(k)}\right) \cdot a_i^{(m+1)}$$

Ceci est $\geq \left(\frac{1}{n}\sum_{i=1}^{n}\prod_{k=1}^{m}a_i^{(k)}\right) \cdot \left(\frac{1}{n}\sum_{i=1}^{n}a_i^{(m+1)}\right) \geq$

$$\geq \left(\frac{1}{n^m}\prod_{k=1}^{m}\sum_{i=1}^{n}a_i^{(k)}\right) \cdot \left(\frac{1}{n}\sum_{i=1}^{n}a_i^{(m+1)}\right)$$

et ceci vaut justement $\frac{1}{n^{m+1}}\prod_{k=1}^{m+1}\sum_{i=1}^{n}a_i^{(k)}$ (cqfd).

UNE GÉNÉRALISATION DU THÉORÈME D'EULER

Dans les paragraphes qui suivent nous allons demontrer un résultat qui remplace le théorème d'Euler:

"Si $(a, m)=1$, alors $a^{\varphi(m)} \equiv 1 (\bmod m)$"

dans le cas où a et m ne sont pas premiers entre eux.

A -Notions introductives.

On suppose $m > 0$. Cette supposition ne nuit pas à la généralité, parce que l'indicatrice d'Euler satisfait l'égalité:

$\varphi(m) = \varphi(-m)$ (cf [1], et que les congruences vérifient la propriété suivante:

$a \equiv b (\bmod m) \Leftrightarrow a \equiv b (\bmod -m)$ (cf [1] pp 12-13).

Quant a la relation de congruence modulo 0, c'est la relation d'égalité. On note (a, b) le plus grand commun diviseur de deux nombres entiers a et b, et on choisit $(a, b)>0$.

B - Lemmes, théorème.

Lemme 1: Soit a un nombre entier et m un naturel > 0. Il existe d_o, m_o de **N** tels que $a = a_o d_o$, $m = m_o d_o$ et $(a_o, m_o)= 1$.

Preuve:

Il suffit de choisir $d_o= (a, m)$. En conformité avec la définition du PGCD, les quotients a_o et m_o de a et m par leur PGCD sont premiers entre eux (of [3] pp 25-26).

Lemme 2: Avec les notations du lemme 1, si $d_o \neq 1$ et si :

$d_o = d_o^1 d_1$, $m_o = m_1 d_1$, $(d_o^1, m_1) = 1$ et $d_1 \neq 1$, alors $d_o > d_1$ et $m_o > m_1$, et si $d_o= d_1$, alors apres un nombre limite de pas i on a $d_o > d_{i+1} = (d_i, m_i)$.

Preuve:

$$(0)\begin{cases} a = a_o d_o & ; \quad (a_o, m_o) = 1 \\ m = m_o d_o & ; \quad d_o \neq 1 \end{cases}$$

$$(1)\begin{cases} d_o = d_o^1 d_1 & ; \quad (d_o^1, m_1) = 1 \\ m_o = m_1 d_1 & ; \quad d_1 \neq 1 \end{cases}$$

De (0) et de (1) il résulte que $a = a_o d_o = a_o d_o^1 d_1$ donc $d_o = d_o^1 d_1$ donc $d_o > d_1$ si $d_o^1 \neq 1$.

De $m_o = m_1 d_1$ on déduit que $m_o > m_1$.

Si $d_o = d_1$ alors $m_o = m_1 d_o = k \cdot d_o^z$ ($z \in \mathbf{N}^*$ et $d_o \nmid k$).

Donc $m_1 = k \cdot d_o^{z-1}$; $d_2 = (d_1, m_1) = (d_o, k \cdot d_o^{z-1})$. Après $i = z$ pas il vient $d_{i+1} = (d_o, k) < d_o$

Lemme 3: Pour chaque nombre entier aet chaque nombre naturel $m > 0$ on peut construire la séquence suivante des relations:

$$(0)\begin{cases} a = a_o d_o & ; \quad (a_o, m_o) = 1 \\ m = m_o d_o & ; \quad d_o \neq 1 \end{cases}$$

$$(1)\begin{cases} d_o = d_o^1 d_1 & ; \quad (d_o^1, m_1) = 1 \\ m_o = m_1 d_1 & ; \quad d_1 \neq 1 \end{cases}$$

....

$$(s\text{-}1)\begin{cases} d_{s-2} = d_{s-2}^1 d_{s-1} & ; \quad (d_{s-2}^1, m_{s-1}) = 1 \\ m_{s-2} = m_{s-1} d_{s-1} & ; \quad d_{s-1} \neq 1 \end{cases}$$

$$(s)\begin{cases} d_{s-1} = d_{s-1}^1 d_s & ; \quad (d_{s-1}^1, m_s) = 1 \\ m_{s-1} = m_s d_s & ; \quad d_s \neq 1 \end{cases}$$

Preuve:

On peut construire cette séquence en appliquant le lemme

1.La séquence est limitée, d'après le lemme 2, car apres r_1 pas on a: $d_o > d_{r_1}$ et $m_o > m_{r_1}$, et après r_2 pas on a: $d_{r_1} > d_{r_1+r_2}$ et $m_{r_1} > m_{r_1+r_2}$, etc..., et les m_i sont des naturels. On arrive à $d_s = 1$ parce que si $d_s \neq 1$ on va construire de nouveau un nombre limité de relations $(s+1), \dots, (s+r)$, avec $d_{s+r} < d_s$.

Théorème: Soient $a, m \in \mathbf{Z}$ et $m \neq 0$. Alors $a^{\varphi(m_s)+s} \equiv a^s \pmod{m}$ ou s et m_s sont les mêmes que dans les lemmes ci-dessus.

Preuve:

Comme dans ce qui précède on peut supposer $m > 0$ sans nuire à la généralité. De la séquence de relations du lemme 3 il résulte que:

$$\begin{array}{l} \quad (0) \qquad (1) \qquad\qquad (2) \qquad\qquad (3)\ (s) \\ a = a_o d_o = a_o d_o^1 d_1 = a_o d_o^1 d_1^1 d_2 = \dots = a_o d_o^1 d_1^1 \dots d_{s-1}^1 d_s \end{array}$$

$$\begin{array}{l} \qquad (0) \qquad (1) \qquad\qquad (2) \qquad\qquad (3)\ (s) \\ \text{et } m = m_o d_o = m_1 d_1 d_o = m_2 d_2 d_1 d_o = \dots = m_s d_s d_{s-1} \dots d_1 d_o \end{array}$$

et $m_s d_s d_{s-1} \dots d_1 d_o = d_o d_1 \dots d_{s-1} d_s m_s$

De (0) il découle que $d_o = (a,m)$, et de (i) que $d_i = (d_{i-1}, m_{i-1})$, ce pour tout i de $\{1,2,\dots,s\}$.

$$d_o = d_o^1 d_1^1 d_2^1 \dots\dots\dots d_{s-1}^1 d_s$$

$$d_1 = d_1^1 d_2^1 \dots\dots\dots d_{s-1}^1 d_s$$

$$\dots\dots\dots\dots$$

$$d_{s-1} = d_{s-1}^1 d_s$$

$$d_{s-1} = d_s$$

Donc $d_o d_1 d_2 \dots d_{s-1} d_s = (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \dots (d_{s-1}^1)^s (d_s^1)^{s+1}$

$$= (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \dots (d_{s-1}^1)^s \text{ car } d_s = 1.$$

Donc $m = (d_o^1)^1 (d_1^1)^2 (d_2^1)^3 \dots (d_{s-1}^1)^s \cdot m_s$; donc $m_s | m$;

(s) (s)

$(d_s, m_s) = (1, m_s)$ et $(d^1_{s-1}, m_s) = 1$

(s-1)

$1 = (d^1_{s-2}, m_{s-1}) = (d^1_{s-2}, m_s d_s)$ donc $(d^1_{s-2}, m_s) = 1$

(s-2)

$1 = (d^1_{s-3}, m_{s-2}) = (d^1_{s-3}, m_{s-1} d_{s-1}) = (d^1_{s-3}, m_s d_s d_{s-1})$,

donc $(d^1_{s-3}, m_s) = 1$

. . . . . .

$1 \overset{(i+1)}{=} (d^1_i, m_{i+1}) = (d^1_i, m_{i+1} d_{i+2}) = (d^1_i, m_{i+3} d_{i+3} d_{i+2}) = \ldots =$

$= (d^1_i, m_s d_s d_{s-1} \ldots d_{i+2})$ donc $(d^1_i, m_s) = 1$, et ce pour tout i de i de $\{0, 1, \ldots, s-2\}$.

. . . . . .

$1 \overset{(0)}{=} (a_o, m_o) = (a_o, d_1 \ldots d_{s-1} d_s m_s)$ donc $(a_o, m_s) = 1$.

Du théorème d'Euler il résulte que:

$(d^1_i)^{\varphi(m_s)} \equiv 1 (\operatorname{mod} m_s)$ pour tout i de $\{0, 1, \ldots, s\}$,

$a_o^{\varphi(m_s)} \equiv 1 (\operatorname{mod} m_s)$

mais $a_o^{\varphi(m_s)} = a_o^{\varphi(m_s)} (d^1_o)^{\varphi(m_s)} (d^1_1)^{\varphi(m_s)} \ldots (d^1_{s-1})^{\varphi(m_s)}$

donc $a^{\varphi(m_s)} \equiv \underbrace{1 \ldots\ldots\ldots 1}_{s+1 \text{ fois}} (\operatorname{mod} m_s)$

$a^{\varphi(m_s)} \equiv 1 (\operatorname{mod} m_s)$.

$a^s_o (d^1_o)^{s-1} (d^1_1)^{s-2} (d^1_2)^{s-3} \ldots (d^1_{s-2})^1 \cdot a^{\varphi(m_s)} \equiv$

$\equiv a^s_o (d^1_o)^{s-1} (d^1_1)^{s-2} \ldots (d^1_{s-2})^1 \cdot 1 (\operatorname{mod} m_s)$

On multiplie par:

$(d^1_o)^1 (d^1_1)^2 (d^1_2)^3 \ldots (d^1_{s-2})^{s-1} (d^1_{s-1})^s$ et on obtient:

$a^s_o (d^1_o)^s (d^1_1)^s \ldots (d^1_{s-2})^s (d^1_{s-1})^s a^{\varphi(m_s)} \equiv$

$\equiv a^s_o (d^1_o)^s (d^1_1)^s \ldots (d^1_{s-2})^s (d^1_{s-1})^s (\operatorname{mod} (d^1_o)^1 \ldots (d^1_{s-1})^s m_s)$

mais $a_o^s(d_o^1)^s(d_1^1)^s\ldots(d_{s-1}^1)^s\cdot a^{\varphi(m_s)}=a^{\varphi(m_s)+s}$ et $a_o^s(d_o^1)^s(d_1^1)^s\ldots(d_{s-1}^1)^s=a^s$ donc $a^{\varphi(m_s)+s}\equiv a^s(\mathrm{mod}\, m)$, pour tous a,m de $\mathbf{Z}(m\neq 0)$

Observations:

(1) Si (a,m)=1 alors $d=1$. Donc $s=0$, et d'après le théorème on a $a^{\varphi(m_o)+0}\equiv a^o(\mathrm{mod}\, m)$ càd $a^{\varphi(m_o)+0}\equiv 1(\mathrm{mod}\, m)$.

Mais $m=m_od_o=m_o\cdot 1=m_o$. Donc:

$a^{\varphi(m)}\equiv 1(\mathrm{mod}\, m)$, et on obtinet le théorème d'Euler.

(2) Soient a et m deux nombres entiers, $m\neq 0$ et $(a,m)=d_o\neq 1$, et $m=m_od_o$. Si $(d_o,m_o)=1$, alors $a^{\varphi(m_o)+1}\equiv a(\mathrm{mod}\, m)$.

En effet, vient du théorème avec $s=1$ et $m_1=m_o$.

Cette relation a une forme semblable au théorème de Fermat:

$a^{\varphi(p)+1}\equiv a(\mathrm{mod}\, p)$

C - UN ALGORITHME POUR RESOUDRE LES CONGRUENCES.

On va construire un algorithme et montrer le schéma logique permettant de calculer s et m_s du théorème.

Données à entrer: deux nombres entiers a et m, $m\neq 0$.

Résultats en sortie: s et m_s ainsi que

$a^{\varphi(m_s)+s}\equiv a^s(\mathrm{mod}\, m)$.

Methode: (1) $A:=a$
$M:=m$
$i:=0$

(2) Calculer $d=(A,M)$ et $M'=M/d$.

(3) Si $d = 1$ prendre $S = i$ et $m_s = M'$ stop.

Si $d \neq 1$ prendre $A := d$, $M = M'$

$i := i+1$, et aller en (2).

Rem: la correction d'algorithme résulte du lemme 3 et du théorème.

Voir organigramme page suivante.

Dans cet organigramme, SUBROUTINE CMMDC calcule $D = (A,M)$ et choisit $D > 0$.

Application: Dans la résolution des exercices on utilise le théorème et l'algorithme pour calculer s et m_s.

Exemple: $6^{25604} \equiv ?$ (mod 105765)

L'on ne peut pas appliquer Fermat ou Euler car (6,105765) = 3 ≠ 1. On appligue donc l'algorithme pour calculer s et m_s et puis le théorème antérieur:

$d_o = (6,105765)=3$ $\qquad$ $m_o = 105765/3 = 35255$

$i = 0$; $3 \neq 1$ donc $i = 0 + 1 = 1$, $d_1 = (3,35255) = 1$,

$m_1 = 35255/1 = 35255$.

Donc $6^{\varphi(35255)+1} \equiv 6^1$ (mod 105765) donc

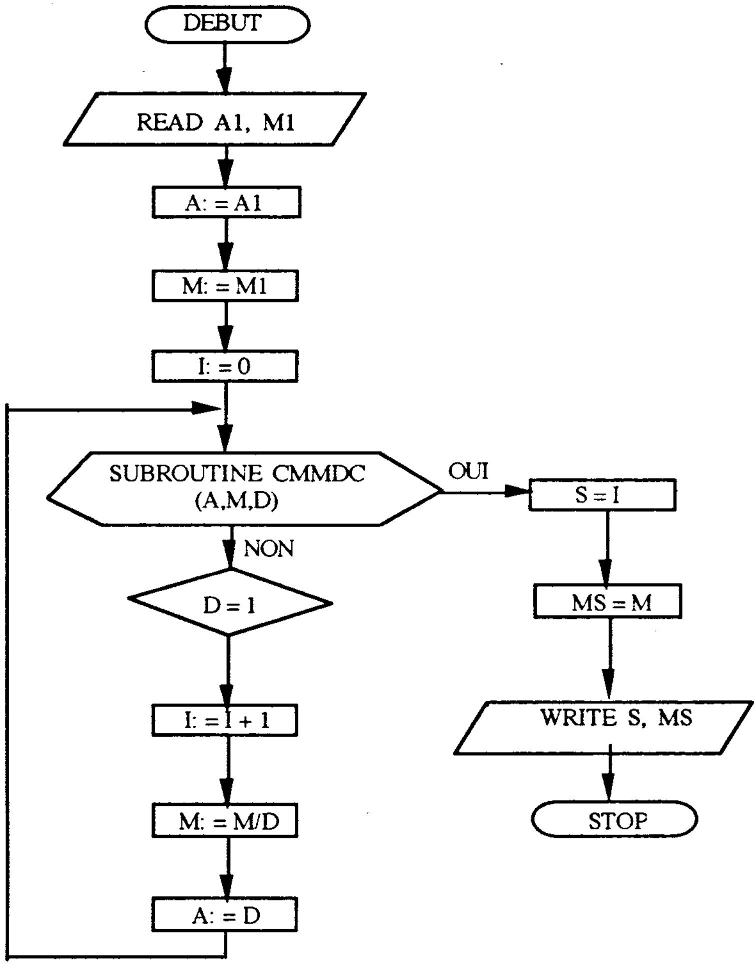
$6^{25604} \equiv 6^4$ (mod 105765).

*

* *

*

Organigramme:



BIBLIOGRAPHIE:

[1] Popovici, Constantin P. - "Teoria numerelor", Curs, Bucarest, Editura didactică şi pedagogică, 1973.

[2] Popovici, Constantin P.- "Logica şi teoria numerelor", Editura didactică şi pedagogică, Bucarest, 197o.

[3] Creangă I, Cazacu C, Mihut P, Opait Gh, Reischer Corina- "Introducerea în teoria numerelor", Editura didactică şi pedagogică, Bucarest, 1965.

[4] Rusu E, - "Arithmetica şi teoria numerelor", Editura didactică şi pedagogică, Ediţia a 2-a, Bucarest, 1963.

[Publie dans le "Bulet.Univ.Braşov", seria C, Vol,XXIII, 1981, pp. 7-12; MR: 84j:1ooo6.]

UNE GENERALISATION DE L'INEGALITE CAUCHY-BOUNIAKOVSKI-SCHWARTZ

Enoncé: Soient les réels $a_i^{(k)}$, $i \in \{1,2,\dots,n\}$, $k \in \{1,2,\dots,m\}$, avec $m \geq 2$. Alors:

$$\left(\sum_{i=1}^{n}\prod_{k=1}^{m} a_i^{(k)}\right)^2 \leq \prod_{k=1}^{m}\sum_{i=1}^{n}\left(a_i^{(k)}\right)^2.$$

Démonstration:

On note A le membre de gauche de l'inegalite et B le membre de droite. On a:

$$A = \sum_{i=1}^{n}\left(a_i^{(1)}\dots a_i^{(m)}\right)^2 + 2\sum_{i=1}^{n-1}\sum_{k=i+1}^{n}\left(a_i^{(1)}\dots a_i^{(m)}\right)\left(a_k^{(1)}\dots a_k^{(m)}\right)$$

et $B = \sum_{(i_1,\dots,i_m)\in E}\left(a_{i_1}^{(1)}\dots a_{i_m}^{(m)}\right)^2$,

où $E = \left\{(i_1,\dots,i_m) \,/\, i_k \in \{1,2,\dots,n\}, 1 \leq k \leq m\right\}$. D'où:

$$B = \sum_{i=1}^{n}\left(a_i^{(1)}\dots a_i^{(m)}\right)^2 + \sum_{i=1}^{n-1}\sum_{k=i+1}^{n}\left[\left(a_i^{(1)}\dots a_i^{(m-1)} a_k^{(m)}\right)^2 + \right.$$

$$\left. + \left(a_k^{(1)}\dots a_k^{(m-1)} a_i^{(m)}\right)^2\right] + \sum_{(i_1,\dots,i_m)\in E-(\Delta_E \cup L^m}\left(a_{i_1}^{(1)}\dots a_{i_m}^{(m)}\right)^2$$

avec $\Delta_E = \left\{(\underbrace{\gamma,\dots,\gamma}_{m \text{ fois}}) \,/\, \gamma \in \{1,2,\dots,n\}\right\}$

et $L = \left\{(\underbrace{\alpha,\dots,\alpha}_{m-1},\beta),(\underbrace{\beta,\dots,\beta}_{m-1},\alpha) \,/\, (\alpha,\beta) \in \{1,2,\dots,n\}^2 \text{et}\, \alpha < \beta\right\}$

Alors

$$A - B = \sum_{i=1}^{n-1} \sum_{k=i+1}^{n} \left[-\left(a_i^{(1)} \dots a_i^{(m-1)} a_k^{(m)} - a_k^{(1)} \dots a_k^{(m-1)} a_i^{(m)} \right)^2 \right] -$$

$$- \sum_{(i_1, \dots, i_m) \in E - (\Delta_E \cup L)} \left(a_{i_1}^{(1)} \dots a_{i_m}^{(m)} \right)^2 \le 0$$

Remarque; pour $m = 2$ on obtient l'inégalité de Cauchy-Bouniakovski-Schwartz.

GENERALISATIONS DU THEOREME DE CÉVA

Dans ces paragraphes on présente trois généralisations du célèbre theoreme de Céva, don l'énoncé est:

"Si dans un triangle ABC on trace les droites concourantes AA_1, BB_1, CC_1 alors $\frac{\overline{A_1B}}{\overline{A_1C}} \cdot \frac{\overline{B_1C}}{\overline{B_1A}} \cdot \frac{\overline{C_1A}}{\overline{C_1B}} = -1$".

Théorème: Soit le polygone $A_1A_2 \ldots A_n$, un point M dans son plan, et une permutation circulaire $p = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix}$. On note M_{ij} les intersections de la droite A_iM avec les droites $A_{i+s}A_{i+s+1}, \ldots, A_{i+s+t-1}A_{i+s+t}$ (pour tous i et j, $j \in \{i+s, \ldots, i+s+t-1\}$).

Si $M_{ij} \neq A_n$ pour tous les indice respectifs, et si $2s+t=n$, on a: $\prod_{i,j=1,i+s}^{n,i+s+t-1} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p}(j)}} = (-1)^n$ (s et t naturels non nuls).

Démonstration analytique: Soit M un point dans le plan du triangle ABC, tel qu il satisfasse aux conditions du théorème. On choisit un système cartesien d'axes, tel que les deux paralleles aux axes qui passent par M ne passent par aucun point A_i (ce qui est posible).

On considère $M(a,b)$, où a et b sont des variables réelles, et $A_i(X_i, Y_i)$, où X_i et Y_i sont connues, $i \in \{1,2,\ldots n\}$.

Le choix anterieur nous assure les relations suivantes:

$X_i - a \neq 0$ et $Y_i - b \neq$ pour tout i de $i \in \{1,2,\ldots n\}$.

L'équation de la droite A_iM ($1 \leq i \leq n$) est:

$$\frac{x-a}{X_i-a}-\frac{y-b}{Y_i-b}$$ On la note $d(x,y;X_i,Y_i)=0$.

On a

$$\frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p(j)}}}=\frac{\delta(A_j,A_iM)}{\delta(A_{p(j)},A_iM)}=\frac{d(X_j,Y_j;X_i,Y_i)}{d(X_{p(j)},Y_{p(j)};X_i,Y_i)}=\frac{D(j,i)}{D(p(j),i)}$$

Où $\delta(A,ST)$ est la distance de A à la droite ST, et ou l'on note $D(a,b)$ pour $d(X_a,Y_a;X_b,Y_b)$.

Calculons le produit, où nous utiliserons la convention suivante: $a+b$ signifiera $\underbrace{p(p(..p}_{b\text{ fois}}(a)..))$ et $a-b$ signifiera

$\underbrace{p^{-1}(p^{-1}(..p^{-1}}_{b\text{ fois}}(a)..))$

$$\prod_{j=i+s}^{i+s+t-1}\frac{\overline{M_{ij}A_j}}{M_{ij}A_{j+1}}=\prod_{j=i+s}^{i+s+t-1}\frac{D(j,i)}{D(j+1,i)}=$$

$$\frac{D(i+s,i)}{D(i+s+1,i)}\cdot\frac{D(i+s+1,i)}{D(i+s+2,i)}\cdots\frac{D(i+s+t-1,i)}{D(i+s+t,i)}=$$

$$\frac{D(i+s,i)}{D(i+s+t,i)}=\frac{D(i+s,i)}{D(i-s,i)}$$

Le produit initial est égal à;

$$\prod_{i=1}^{n}\frac{D(i+s,i)}{D(i-s,i)}=\frac{D(1+s,1)}{D(1-s,1)}\cdot\frac{D(2+s,2)}{D(2-s,2)}\cdots\frac{D(2s,s)}{D(n,s)}\cdot$$

$$\cdot\frac{D(2s+2,s+2)}{D(2,s+2)}\cdots\frac{D(2s+t,s+t)}{D(t,s+t)}\cdot\frac{D(2s+t+1,s+t+1)}{D(t+1,s+t+1)}\cdot$$

$$\cdot\frac{D(2s+t+2,s+t+2)}{D(t+2,s+t+2)}\cdots\frac{D(2s+t+s,s+t+s)}{D(t+s,s+t+s)}=$$

$$=\frac{D(1+s,1)}{D(1,1+s)}\cdot\frac{D(2+s,2)}{D(2,2+s)}\cdots\frac{D(2s+t,s+t)}{D(s+t,2s+t)}\cdots\frac{D(s,n)}{D(n,s)}=$$

$$=\prod_{i=1}^{n}\frac{D(i+s,i)}{D(i,i+s)}=\prod_{i=1}^{n}\left(-\frac{P(i+s)}{P(i)}\right)=(-1)^n$$ parce que:

$$\frac{D(r,p)}{D(p,r)} = \frac{\dfrac{X_r - a}{X_p - a} - \dfrac{Y_r - b}{Y_p - b}}{\dfrac{X_p - a}{X_r - a} - \dfrac{Y_p - b}{Y_r - a}} = -\frac{(X_r - a)(Y_r - b)}{(X_p - a)(Y_p - b)} = -\frac{P(r)}{P(p)},$$

la dernière égalité résultant de ce que l'on note: $(X_t - a)(Y_t - b) = P(t)$. De (1) il résulte que $P(t) \neq 0$ pour tout t de $\{1,2,\dots n\}$. La démonstration est terminée.

Commentaires sur le théorème:

t représente le nombre des droites du poygone qui sont coupées par une droite $A_{i_o}M$; si on note les côtés A_iA_{i+1} du polygone a_i, alors $s+1$ représente l'ordre de la première droite coupée par la droite A_1M (c'est a_{s+1} la premiere droite coupee par A_1M).

Exemple: Si $s = 5$ et $t = 3$, le théorème dit que:

- la droite A_1M coupe les côtés A_6A_7, A_7A_8, A_8A_9.
- la droite A_2M coupe les côtés $A_7A_8, A_8A_9, A_9A_{10}$.
- la droite A_3M coupe les côtés $A_8A_9, A_9A_{10}, A_{10}A_{11}$ etc...

Observation: la condition restrictive du théorème est nécessaire pour l'existence des rapports $\dfrac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p}(j)}}$.

Conséquence 1: Soient un polygone $A_1A_2\dots A_{2k+1}$ et un point M dans son plan. Pour tout i de $\{1,2,\dots,2k+1\}$, on note M_i l'intersection de la droite $A_iA_{p(i)}$ avec la droite qui passe par M et par le sommet opposé à cette droite. Si $M_i \notin \{A_i, A_{p(i)}\}$ alors on a: $\displaystyle\prod_{i=1}^{n} \frac{\overline{M_iA_i}}{M_iA_{p(i)}} = -1.$

La démonstration résulte immédiatement du théorème, puisqu' on a $s = k$ et $t = 1$, c'est-à-dire $n = 2k + 1$.

La réciproque de cette conséquenee n'est pas vraie.

D'ou il resulte immediatement que la reciproque du théorèma n'est pas non plus vraie.

Contre-exemple:

On considere un polygone de 5 côtés. On trace les droites A_1M_3, A_2M_4 et A_3M_5 concourantes en M.

Soit $K = \dfrac{\overline{M_3A_3}}{\overline{M_3A_4}} \cdot \dfrac{\overline{M_4A_4}}{\overline{M_4A_5}} \cdot \dfrac{\overline{M_5A_5}}{\overline{M_5A_1}}$

Puis on trace la droite A_4M_1 telle qu'elle ne passe pas par M et telle qu'elle forme le rapport: (2)

$\dfrac{\overline{M_1A_1}}{\overline{M_1A_2}} = 1/K$ ou $2/K$. (on choisit l'une de ces valeurs, pour que A_4M_1 ne passe pas par M).

A la fin on trace A_5M_2 qui forme le rapport $\dfrac{\overline{M_2A_2}}{\overline{M_2A_3}} = -1$ ou $-\dfrac{1}{2}$ en fonction de (2). Donc le produit:

$\prod_{i=1}^{5} \dfrac{\overline{M_iA_i}}{\overline{M_iA_{p(i)}}}$ sans que les droites respectives soient concourantes.

Consequence 2: Dans les conditions du théorème, si pour tout i et $j, j \notin \{i, p^{-1}(i)\}$, on note $M_{ij} = A_iM \cap A_jA_{p(j)}$ et $M_{ij} \notin \{A_j, A_{p(j)}\}$ alors on a:

$$\prod_{\substack{i,j=1 \\ j \notin \{i, p^{-1}(i)\}}}^{n} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{p(j)}}} = (-1)^n.$$

En effet on a $s = 1$, $t = n - 2$, et donc $2s + t = n$.

Consequence 3: Pour $n = 3$, il vient $s = 1$ et $t = 1$, cad on obtient (comme cas particulier) le théorème de Céva.

UNE APPLICATION DE LA GÉNÉRALISATION DU THÉORÈME DE CÉVA

Théorème: Soit un polygone $A_1A_2\dots A_n$ inscrit dans un cercle. Soient s et t deux naturels non nuls tels que $2s+t=n$. Par chaque sommet A_i passe une droite d_i qui coupe les droites $A_{i+s}A_{i+s+1},\dots,A_{i+s+t-1}A_{i+s+t}$ aux points $M_{i,i+s}$, ... , respectivement $M_{i+s+t-1}$ et le cercle au point M_i'. Alors on a:

$$\prod_{i=1}^{n}\prod_{j=i+s}^{i+s+t-1}\frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{j+1}}}=\prod_{i=1}^{n}\frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+t}}}.$$

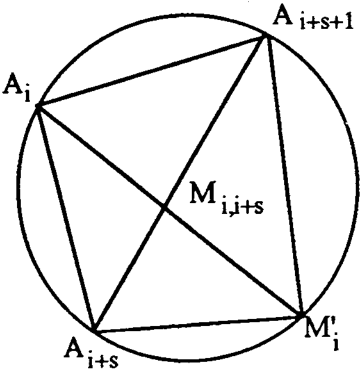
Preuve:

Soit i fixé.

1) Cas où le point $M_{i,i+s}$ se trouve à l'interieur du cercle:

On a les triangles $A_iM_{i,i+s}A_{i+s}$ et $M_i'M_{i,I+S}A_{i+s+1}$ semblables, puisque les angles $M_{i,i+s}A_iA_{i+s}$ et $M_{i,i+s}A_{i+s+1}M_i'$ d'une part, et $A_iM_{i,i+s}A_{i+s}$ et $A_{i+s+1}M_{i,i+s}M_i'$ sont égaux. Il en résulte que:

$$\frac{\overline{M_{i,i+s}A_i}}{\overline{M_{i,i+s}A_{i+s+1}}}=\frac{\overline{A_iA_{i+s}}}{\overline{M_i'A_{i+s+1}}}.$$

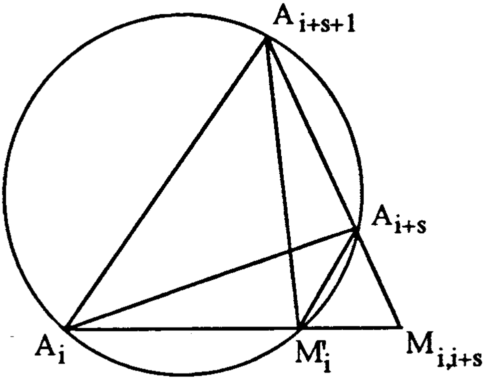


De manière analogue, on montre que les triangles $M_{i,i+s}A_iA_{i+s+1}$ et $M_{i,i+s}A_{i+s}M_i'$ sont semblables, d'où:

(2) $\dfrac{\overline{M_{i,i+s}A_i}}{\overline{M_{i,i+s}A_{i+s}}} = \dfrac{\overline{A_iA_{i+s+1}}}{\overline{M_i'A_{i+s}}}$. On divise (1) par (2) et on obtient:

$$(3)\quad \frac{\overline{M_{i,i+s}A_{i+s}}}{\overline{M_{i,i+s}A_{i+s+1}}} = \frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+1}}} \cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+1}}}.$$

2) Le cas où $M_{i,i+s}$ est exterieur au cercle est similaire au premier, parce que les triangles (notes comme au 1) sont semblables aussi dans ce nouveau cas. On a les mêmes raisonnements et les mêmes raports, donc on a aussi la relation (3).



Calculons le produit:

$$\prod_{j=i+s}^{i+s+t-1} \frac{\overline{M_{ij}A_j}}{\overline{M_{ij}A_{j+1}}} = \prod_{j=i+s}^{i+s+t-1} \left(\frac{\overline{M_i'A_j}}{\overline{M_i'A_{j+1}}} \cdot \frac{\overline{A_iA_j}}{\overline{A_iA_{j+1}}} \right) =$$

$$= \frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+1}}} \cdot \frac{\overline{M_i'A_{i+s+1}}}{\overline{M_i'A_{i+s+2}}} \cdots \frac{\overline{M_i'A_{i+s+t-1}}}{\overline{M_i'A_{i+s+t}}} \cdot$$

$$\frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+1}}} \cdot \frac{\overline{A_iA_{i+s+1}}}{\overline{A_iA_{i+s+2}}} \cdots \frac{\overline{A_iA_{i+s+t-1}}}{\overline{A_iA_{i+s+t}}} = \frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+t}}} \cdot \frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}}$$

Donc le produit initial est égal à:

$$\prod_{i=1}^{n}\left(\frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+t}}}\cdot\frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}}\right)=\prod_{i=1}^{n}\frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+t}}}$$

puisque:

$$\prod_{i=1}^{n}\frac{\overline{A_iA_{i+s}}}{\overline{A_iA_{i+s+t}}}=\frac{\overline{A_1A_{1+s}}}{\overline{A_1A_{1+s+t}}}\cdot\frac{\overline{A_2A_{2+s}}}{\overline{A_2A_{2+s+t}}}\cdots\frac{\overline{A_sA_{2s}}}{\overline{A_{s+1}A_1}}\cdot$$

$$\cdot\frac{\overline{A_{s+2}A_{2s+2}}}{\overline{A_{s+2}A_2}}\cdots\frac{\overline{A_{s+t}A_n}}{\overline{A_{s+t}A_t}}\cdot\frac{\overline{A_{s+t+1}A_1}}{\overline{A_{s+t+1}A_{t+1}}}\cdot\frac{\overline{A_{s+t+2}A_2}}{\overline{A_{s+t+2}A_{t+2}}}\cdots\frac{\overline{A_nA_s}}{\overline{A_nA_{s+t}}}=1$$

(en tenant compte du fait que $2s+t=n$).

Conséquence 1: Si on a un polygone $A_1A_2\ldots A_{2s-1}$ inscrit dans un cercle, et que de chaque sommet A_i on trace une droite d_i qui coupe le côté opposé $A_{i+s-1}A_{i+s}$ en M_i et le cercle en M_i' alors:

$$\prod_{i=1}^{n}\frac{\overline{M_iA_{i+s-1}}}{\overline{M_iA_{i+s}}}=\prod_{i=1}^{n}\frac{\overline{M_i'A_{i+s-1}}}{\overline{M_i'A_{i+s}}}$$

En effet pour $t=1$, on a n impair et $s=\dfrac{n+1}{2}$.

Si on fait $s=1$ dans cette coséquence, on retrouve la note mathématique de [1], pages 35-37.

Application: si dans le théorème, les droites d_i sont concourantes, on obtient:

$$\prod_{i=1}^{n}\frac{\overline{M_i'A_{i+s}}}{\overline{M_i'A_{i+s+t}}}=(-1)^n$$ (Pour cela, voir [2]).

Bibliographie:

[1] Dan Barbilian, Ion Barbu -"Pagini inedite", Editura Albatros, Bucarest, 1981 (Ediție ingrijită de Gerda Barbilian, V.Protopopescu, Viorel Gh.Vodă).

[2] Florentin Smarandache -"Généralisation du théorème de Céva".

UNE GÉNÉRALISATION D'UN THÉORÈME DE CARNOT

Théorème de Carnot: Sont un point M sur la diagonale AC d'un quadrilatère quelconque $ABCD$. Par M on trace une droite qui coupe AB en α et BC en β. Puis on trace une autre droite, qui coupe CD en γ et AD en δ. Alors on a:

$$\frac{A\alpha}{B\alpha}\cdot\frac{B\beta}{C\beta}\cdot\frac{C\gamma}{D\gamma}\cdot\frac{D\delta}{A\delta}=1.$$

Généralisation: Soit un polygone $A_1\ldots A_n$. Sur une diagonale A_1A_k de celui-ci on prend un point M par lequel on trace une droite d_1 qui coupe les droites $A_1A_2, A_2A_3, \ldots, A_{k-1}A_k$ respectivement aux points $P_1, P_2, \ldots, P_{k-1}$ et une autre droite d_2 coupe les autres droites $A_kA_{k+1}, \ldots, A_{n-1}A_n, A_nA_1$ respectivement aux points $P_k, \ldots, P_{n-1}, P_n$. Alors on a:

$$\prod_{i=1}^{n}\frac{A_iP_i}{A_{\varphi(i)}P_i}=1,$$ où φ este la permutation circulaire

$$\begin{pmatrix}1 & 2 & \ldots & n-1 & n\\ 2 & 3 & \ldots & n & 1\end{pmatrix}.$$

Démonstration:

Soit $1\le j\le k-1$ On montre facilement que:

$$\frac{A_jP_j}{A_{j+1}P_j}=\frac{D(A_j,d_1)}{D(A_{j+1},d_1)}$$ où $D(A,d)$ représente la distance du point A à la droite d, puisque les triangles $P_jA_jA'_j$ et $P_jA_{j+1}A'_{j+1}$ sont semblables. (On note A'_j et A'_{j+1} les projections das points A_j et A_{j+1} sur la droite d_1).

Il en resulte que:

$$\frac{A_1P_1}{A_2P_1}\cdot\frac{A_2P_2}{A_3P_2}\cdots\frac{A_{k-1}P_{k-1}}{A_kP_{k-1}}=\frac{D(A_1,d_1)}{D(A_2,d_1)}\cdot\frac{D(A_2,d_1)}{D(A_3,d_1)}\cdots\frac{D(A_{k-1},d_1)}{D(A_k,d_1)}$$
$$=\frac{D(A_1,d_1)}{D(A_k,d_1)}$$

De manière analogue, pour $k \leq h \leq n$ on a:

$$\frac{A_hP_h}{A_{\varphi(h)}P_h}=\frac{D(A_d,d_2)}{D(A_{\varphi(h)},d_2)} \text{ et } \prod_{h=k}^{n}\frac{A_hP_h}{A_{\varphi(h)}P_h}=\frac{D(A_k,d_2)}{D(A_1,d_2)}.$$

Le produit du théorème est égal à:

$\dfrac{D(A_1,d_1)}{D(A_k,d_1)}\cdot\dfrac{D(A_k,d_2)}{D(A_1,d_2)}$, mais $\dfrac{D(A_1,d_1)}{D(A_k,d_1)}=\dfrac{A_1M}{A_kM}$ puisque les triagles MA_1A_1' et MA_kA_k' sont semblables. De même, puisque les triangles MA_1A_1'' et MA_kA_k'' sont semblables (on note A_1'' et A_k'' les projections respectives de A_1 et A_k sur la droite d_2), on a :

$$\frac{D(A_k,d_2)}{D(A_1,d_2)}=\frac{A_kM}{A_1M}$$

Le produit de l'énoncé est donc bien égal à 1.

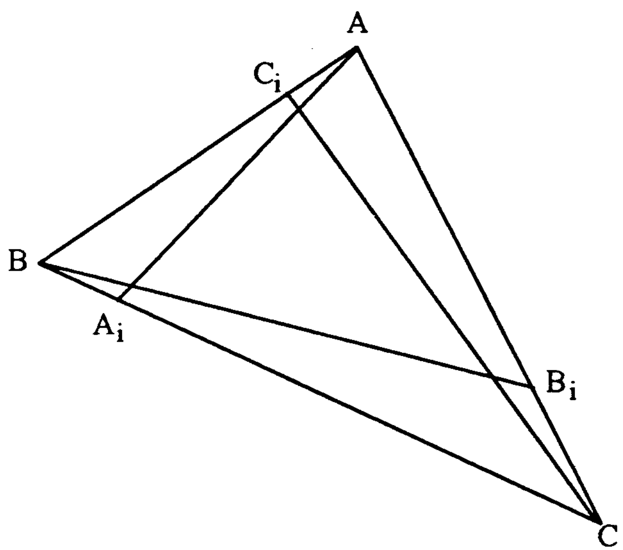
Rem: si on remplace n par 4 dans ce théorème, on retrouve le théorème de Carnot.

QUELQUES PROPRIETES DES NEDIANES

Cet article généralise ceratins résultats sur les nédianes (voir [1] p. 97-99). On appelle *nédianes* les segments de droite qui passent par un sommet du triangle et partagent le côté oppesé en n parties égales. Une nédiane est appelée d'ordre i si elle partage le côté opposé dans le rapport i / n.

Pour $1 \le i \le n-1$ les nédianes d'ordre i (c'est-à-dire AA_i, BB_i et CC_i) ont les propriétés suivantes:

1) Avec ces 3 segments on peut construire un triangle.



2) $|AA_i|^2 + |BB_i|^2 + |CC_i|^2 = \dfrac{i^2 - i \cdot n + n^2}{n^2}(a^2 + b^2 + c^2)$.

Preuves.

$$\overrightarrow{AA_i} = \overrightarrow{AB} + \overrightarrow{BA_i} = \overrightarrow{AB} + \frac{i}{n}\overrightarrow{BC} \quad (1)$$

$$\overrightarrow{BB_i} = \overrightarrow{BC} + \overrightarrow{CB_i} = \overrightarrow{BC} + \frac{i}{n}\overrightarrow{CA} \quad (2)$$

$$\overrightarrow{CC_i} = \overrightarrow{CA} + \overrightarrow{AC_i} = \overrightarrow{CA} + \frac{i}{n}\overrightarrow{AB} \quad (3)$$

En additionnant ces 3 relations, il vient:

$\overrightarrow{AA_i} + \overrightarrow{BB_i} + \overrightarrow{CC_i} = \frac{i+n}{n}(\overrightarrow{AB} + \overrightarrow{BC} + \overrightarrow{CA}) = 0$ donc les 3 nédianes peuvent être les cotés d'un triangle.

(2) En élevant au carré les 3 relations et en faisant la somme on obtient:

$$|AA_i|^2 + |BB_i|^2 + |CC_i|^2 = a^2 + b^2 + c^2 + \frac{i^2}{n^2}(a^2 + b^2 + c^2) +$$

$$+ \frac{i}{n}(2\overrightarrow{AB}\cdot\overrightarrow{BC} + 2\overrightarrow{BC}\cdot\overrightarrow{CA} + 2\overrightarrow{CA}\cdot\overrightarrow{AB}) \quad (4)$$

Puisque $2\overrightarrow{AB}\cdot\overrightarrow{BC} = -2ca\ \cos B = b^2 - c^2 - a^2$ (th. du cosinus), en reportant ceci dans la relation (4) on a la relation cherohée.

Bibliographie:

[1] Voda, Dr, Viorel Gh. -"Surprize în matematica elementară", Editura Albatros,Cucarest, 1981.

GENERALIZĂRI ALE TEOREMEI LUI DESARGUES*

Se dau punctele $A_1,\ldots,A_n$ situate în același plan și $B_1,\ldots,B_n$ situate în alt plan, astfel încât dreptele A_iB_i să fie concurente. Să se arate că dreptele A_iA_j și B_iB_j sunt concurente, atunci punctele lor de intersecție sunt coliniare.

Soluție. Notăm cu α un plan care conține punctele $A_1,\ldots,A_n$ (în cazul în care punctele sunt necoliniare α este unic) iar analog $\beta = P(B_1,\ldots,B_n)$ și considerăm $\alpha \cap \beta = d$. Deoarece dreptele A_iA_j și B_iB_j sunt concurente, iar $A_iA_j \subset \alpha$ și $B_iB_j \subset \beta$ deci intersecția lor aparține dreptei d.

OBSERVAȚIA 1. Pentru $n = 3$ și A_1, A_2, A_3 necoliniare, B_1, B_2, B_3 necoliniare iar $A_i \neq B_j$ se obține teorema lui Desarques.

OBSERVAȚIE 2. O generalizare a acestei generalizări este Se dau punctele $A_1,\ldots,A_n$ situate într-un plan, iar $B_1,\ldots,B_m$ situate în alt plan. Să se arate că, dacă A_iA_j și B_kB_r sunt concurente, atunci punctele lor de intersecție sunt concurente.

OBSERVAȚIA 3. Pentru $n = m$, iar dreptele A_iB_i concurente se obține prima generalizare.

OBSERVAȚIA 4. Dacă în plus mai avem $n = m = 3$ precum și condițiile anterioare găsim teorema lui Desarques.

---

* Gamma, anul X, nr. 1-2, oct. 1987.

COEFFCIENTS K-NOMIAUX

Dans cet article on élargit les notions de " coefficients binomiaux" et de "coefficients trinomiaux" à la notion de "coiefficients k-nomiaux", et on obient quelques propiétés général de ceux-ci. Comme aplication, on généralisera le "triangle de Pascal".

On considère ub nombre naturel $k \geq 2$; soit $P(x) = 1 + x + x^2 + \ldots + x^{k-1}$ le polynôme formé de k monômes de ce type; on l'appellera "k-nôme".

On appelle *coefficients k-nomiaux* les coefficients des puissances de x de $(1 + x + x^2 + \ldots + x^{k-1})^n$, pour n entier positif. On les notera Ck_n^h avec $h \in \{0,1,2,\ldots,2pn\}$

Par la suite on va construire par récurrence un triangle de nombres qui va être applé *"triangle des nombres d'ordre k"*.

CAS 1 : $k = 2p + 1$.

Sur la première ligne du triangle on écrit 1 et on l'appelle "ligne 0".

(1) On convient que toutes les cases qui se trouvent a gauche et à droit du premier (respectivement du dernier) nombre de chaque ligne seront considérées comme contenent 0. Les lignes suivantes sont appellées "ligne 2 ", etc... Chaque ligne contiendra 2P nombres à gauche du premier nombre, p nombres à droite du dernier nombre de la ligne précédente. Les nombres de la ligne $i + 1$ s'obtiennent à partir de ceoux de la ligne i de la façon suivante :

Ck_{i+1}^j este égal a l'addition des p nombres situés à sa gauche sur la ligne i et des p nombres situés à sa droite sur la ligne i, au nombre situé au-dessus de lui (voir fig. 1). On va tenir compte de la convention 1.

Fig.1: ligne i $\quad \overbrace{\cdots\cdots}^{p \text{ nombres}} \quad \cdot \quad \overbrace{\cdots\cdots}^{p \text{ nombres}}$

ligne $i+1$ $\quad \cdot\, Ck_{i+1}^{j}$

Exemple pour $k=5$:

1

1 1 1 1 1

1 2 3 4 5 4 3 2 1

1 3 6 10 15 18 19 18 15 10 6 3 1

1 4 10 20 35 52 68 80 85 80 68 52 35 20 10 4 1

....

Le nombre $C5_1^0 = 0+0+0+0+1 = 1$; $C5_1^3 = 0+1+0+$ $+0+0 = 1$, $C5_2^3 = 0+1+1+1+1 = 4$; $C5_3^7 = 4+5+4+$ $3+2 = 18$, etc...

Propriétés du triangle, de nombres d'ordre k:

1) La ligne i a $2pi+1$ éléments.

2) $Ck_n^h = \sum_{i=0}^{2p} Ck_{n-1}^{h-i}$ où par convention $Ck_n^t = 0$ pour $\begin{cases} t<0 & \text{et} \\ t>2pr \end{cases}$

Ceci est évident d'après la construction du triangle.

3) Chaque ligne est symétrique par rapport à l'élément cetral.

4) Les premiers éléments de la ligne i sont 1 et i.

5) La ligne i du triangle de nombres d'ordre k représente les coefficients k-nomiaux de $(1+x+x^2+\ldots+x^{k-1})^i$.

La démonstration se fait par récurrence sur i de $\mathbf{N}^*$:

a) Pour $i=1$ c'est évident; (on fait la propriété serait encore vraie pour $i=0$).

b) Supposons la propriété vraie pour n. Alors

$$(1+x+x^2+\ldots+x^{k-1})^{n+1} =$$

$$= (1+x+x^2+\ldots+x^{k-1})(1+x+x^2+\ldots+x^{k-1})^n =$$

$$= (1+x+x^2+\ldots+x^{2p}) \cdot \sum_{j=0}^{2pn} Ck_n^j \cdot x^j =$$

$$= \sum_{t=0}^{2p(n+1)} \sum_{\substack{i+j=t \\ 0\le j\le 2p \\ 0\le i\le 2pn}} Ck_n^i \cdot x^i \cdot x^j =$$

$$= \sum_{t=0}^{2p(n+1)} \left(\sum_{j=0}^{2p} Ck_n^{t-j} \right) x^t = \sum_{t=0}^{2p(n+1)} Ck_{n+1}^t \cdot x^t$$

6) La somme des éléments situés sur la ligne n est égale à, k^n.

La première méthode de démonstration utilise le raisonnement par récurrence. Pour $n = 1$ l'assertion est évidente. On suppose la propriété vraie pour n, c'est-à-dire que la somme des éléments situés sur la ligne n est égale à k^n. La ligne $n+1$ se calcule à partir des éléments de la ligne n. Chaque élément de la ligne n fait partie de la somme qui cacule chacum des p éléments situés à sa gauche sur la ligne $n+1$, chacun des p éléments situés à sa droite sur la ligne $n+1$ et celui qui est situé en dessous: donc il est utilisé pour calculer k nombres de la ligne $n+1$.

Doc la somme des éléments de la ligne $n+1$ est k fois plus grande que la somme de ceux de la ligne n, donc elle vaut k^{n+1}

7) La différence entre la somme des coefficients $k-$nomiaux de rang pair et la somme des coefficients $k-$nomiaux impair situés sur la même ligne ($Ck_n^0 - Ck_n^1 + Ck_n^2 - Ck_n^3 + \ldots$) est égale à 1.

On l'obtient si dans $(1+x+x^2+...+x^{k-1})^n$ on prend $x=-1$.

8) $Ck_n^0 \cdot Ck_m^h + Ck_n^1 \cdot Ck_m^{h-1} + ... + Ck_n^h \cdot Ck_m^0 = Ck_{n+m}^h$

Ceci résulte de ce que, dans l'identité

$$(1+x+x^2+...+x^{k-1})^n \cdot (1+x+x^2+...+x^{k-1})^m =$$
$$= (1+x+x^2+...+x^{k-1})^{n+m}$$

le coefficient de x^h dans le membre de gauch est $\sum_{i=0}^{h} Ck_n^i \cdot Ck_m^{h-i}$ et celui de x^h a droite est Ck_{n+m}^h

9) La somme des carrés des coefficients k-nomiaux situés sur la ligne n est égale au cefficient k-nomial situé au milieu de la ligne $2n$.

Pour la preuve on prend $n = m = h$ dans la propriété 8.

On peut trouver beaucoup de propriétés et applications de ces coefficienst k-nomiaux parce qu'ils élargissent les coefficients binomiaux dont les applications sont connues.

CAS 2 : $k = 2p$.

La construction du triangle de nombres d'ordre k est analogue:

Sur la première ligne on ecrit 1; on l'appelle ligne 0.

Les lignes suivantes sont appelées ligne 1, ligne 2, etc... Chaque ligne aura $2p-1$ éléments de plus la précédente; comme $2p-1$ est un nombre impar, les éléments de chaque ligne seront placés entre les éléments de la ligne précédente (a la différence du cas 1 où ils se plaçaient en-dessous).

Les éléments situés sur la ligne $i+1$ s'obtiennent en utilisant ceux de la ligne i de la façon suivante:

Ck_{i+1}^j est égal à l'addition des p éléments situes à sa gauche sur la ligne i aux p éléments situés à sa droite sur la ligne i.

$$\begin{array}{lcc} & \text{p nbres} & \text{p nbres} \\ \text{Fig.2: ligne } i & \overbrace{\cdot \ldots\ldots \cdot} & \overbrace{\cdot \ldots\ldots \cdot} \\ \quad\text{ligne } i+1 & & \cdot\, Ck_{i+1}^{j} \end{array}$$

Exemple pour $k = 4$:

$$\begin{array}{c} 1 \\ 1 \quad 1 \quad 1 \quad 1 \\ 1 \quad 2 \quad 3 \quad 4 \quad 3 \quad 2 \quad 1 \\ 1 \quad 3 \quad 6 \quad 10 \quad 12 \quad 12 \quad 10 \quad 6 \quad 3 \quad 1 \\ 1 \quad 4 \quad 10 \quad 20 \quad 31 \quad 40 \quad 44 \quad 40 \quad 31 \quad 20 \quad 10 \quad 4 \quad 1 \end{array}$$

....

D'où la propriété 1' : $Ck_n^h = \sum_{i=0}^{2p-1} Ck_{n-1}^{h-i}$

En réunissant les propriétés 1 et 1' : $Ck_n^h = \sum_{i=0}^{k-1} Ck_{n-1}^{h-i}$

Les autres propriétés du Cas 1 se conservent dans le cas 2, avec des preuves analogues. Cependant dans la propriété 7, on voit que la différence entre la somme des coefficients k-nomiaux de rang pair et celle des coefficients k-nomiaux de rang impair situés sur la même ligne est égale à 0.

UNE CLASSE D'ENSEMBLES RÉCURSIFS

Dans cet article on construit une classe d'ensembles récursifs, on établit des propriétés de ces ensembles et on propose des applications. Cet article élargit quelques résultats de [1].

1) Definitions, propriétés.

On appelle esembles récursifs les ensembles d'éléments qui se construisent de manière récursive: soit T un ensemble d'éléments et f_i pour i compris entre 1 et s, des opérations n_i -aires, càd que $f_i: T^{n_i} \to T$. Construisons récursivement l'ensemble M inclus dans T et tel que:

(déf.1) 1°) certains éléments $a_1, \dots, a_n$ de T, appartiennent à M.

2°) si $\alpha_{i_1}, \dots, \alpha_{i_{n_i}}$ appartiennent à M, alors $f_i(\alpha_{i_1}, \dots, \alpha_{i_{n_i}})$ appartient à M pour tout $i \in \{1, 2, \dots, s\}$.

3°) chaque élément de M s'obtient en appliquant un nombre fini de fois les règles 1° ou 2°.

Nous allons démontrer plusieurs propriétés de ces ensembles M, qui découlent de la façon dont ils ont été définis.

L'ensemble M est le représentant d'une classe d'ensembles récursifs parce que dans les régles 1° et 2°, en particularisant les éléments $a_1, \dots, a_n$ respectivement $f_1, \dots, f_s$ on obtient des ensembles différents.

Observation 1: Pour obtenir un élémnt de M, il faut nécessairement appliquer d'abord la régle 1.

(déf.2) Les éléments de M s'appellent éléments M-récursifs.

(déf.3) On appelle ordre d'un élément a de M le plus petit naturel $p \geq 1$ qui a la propriété que a s'obtient en appliquant p fois les règles 1° ou 2°.

On note M_p l'ensemble qui contient tous les éléments d'ordre p de M. Il est évident que $M_1 = \{a_1, \ldots, a_n\}$.

$$M_2 = \bigcup_{i=1}^{s} \left\{ \bigcup_{(\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}) \in M_1^{n_i}} f_i(\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}) \right\} \setminus M_1 .$$

On soustrait M_1 car il est possible que $f_j(a_{j_1}, \ldots, a_{j_{n_j}}) = a_i$ qui appartient à M_1, et donc pas à M_2.

On démontre que pour $k \geq 1$ on a :

$$M_{k+1} = \bigcup_{i=1}^{s} \left\{ \bigcup_{(\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}) \in \prod_k^{(i)}} f_i(\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}) \right\} \setminus \bigcup_{h=1}^{k} M_h$$

où chaque $\prod_k^{(i)} = \Big\{ (\alpha_{i_1}, \ldots, \alpha_{i_{n_i}}) \,/\, \alpha_{i_j} \in M_{q_j} \quad j \in \{1, 2, \ldots, n_i\};$

$1 \leq q_j \leq k$ et au moins un élément $\alpha_{i_{j_o}} \in M_k, 1 \leq j_o \leq n_i \Big\}$.

Les ensembles M_p, $p \in \mathbb{N}^*$ forment une partition de l'ensemble M.

Théorème 1:

$$M = \bigcup_{p \in \mathbb{N}^*} M_p, \text{ où } \mathbb{N}^* = \{1, 2, 3, \ldots\}.$$

Preuve:

De la règle 1° il résulte que $M_1 \subseteq M$.

On suppose que cette propriété est vraie pour des valeurs inférieures à p. Il en résulte que $M_p \subseteq M$, parce que M_p est

obtenu en appliquant la règle 2º aux éléments de $\bigcup_{i=1}^{p-1} M_i$

Donc $\bigcup_{p\in N^*} M_p \subseteq M$. Réciproquement, on a l'inclusion en sens contraire en accord avec la règle 3º.

Théorème 2: L'ensemble M est le plus petit ensemble qui ait les proprietes 1º et 2º.

Preuve:

Soit R le plus petit ensemble ayant les proprietes 1º et 2º. On va démontrer que ce ensemble est unique.

Supposons qu'il existe un autre ensemble R' ayant les propriétés 1º et 2º qui soit le plus petit. Comme R est le plus petit ensemble ayant ces propriétés, et puisque R' les possède aussi, il en résulte que $R \subseteq R'$ de manière analogue, il vient $R' \subseteq R$: donc $R = R'$.

Il est évident que $M_1 \subseteq R$. On suppose que $M_i \subseteq R$ pour $1 \leq i < p$. Alors (règle 3º), et en tenant compte du fait que chaque élément de M_p est obtenu en appliquant la règle 2º à certains éléments de M_i, $1 \leq i < p$ il en résulte que $M_p \subseteq R$. Donc $\bigcup_p M_p \subseteq R (p \in N^*)$, càd $M \subseteq R$. Et comme R est unique, $M = R$.

Observation 2. Le théorème 2 remplace la règle 3º de la définition récursive de l'ensemble M par : "M est le plus petit ensemble satisfaisant les propriétés 1º et 2º".

Théorème 3: M est l'intersection de tous les ensembles de T qui satisfont aux condition 1º et 2º.

Preuve: soit T_{12} la famille de tous les ensembles de T satisfaisant les conditions 1° et 2°. Soit $I = \bigcap_{A \in T_{12}} A$.

I a les propriétés 1° et 2° parce que:

1) Pour tout $i \in \{1,2,\ldots,n\}$, $a_i \in I$, parce que $a_i \in A$ pour tout A de T_{12}.

2) Si $\alpha_{i_1},\ldots,\alpha_{i_{n_i}} \in I$, il en résulte que $\alpha_{i_1},\ldots,\alpha_{i_{n_i}}$ appartiennent à A quel que soit A de T_{12}. Donc, $\forall i \in \{1,2,\ldots,s\}$, $f_i(\alpha_{i_1},\ldots,\alpha_{i_{n_i}}) \in A$ quel que soit A de T_{12}, donc $f_i(\alpha_{i_1},\ldots,\alpha_{i_{n_i}}) \in I$ pour tout i de $\{1,2,\ldots,s\}$.

Du théorème 2 il résulte que $M \subseteq I$.

Puisque M remplit les conditions 1° et 2°, il en résulte que $M \in T_{12}$, d'où $I \subseteq M$. Donc $M = I$.

Déf.) Un ensemble $A \subseteq I$ est dit fermé pour l'operation f_{i_o} ssi pour tout $\alpha_{i_o 1},\ldots,\alpha_{i_o n_{i_o}}$ de A, on a: $f_{i_o}(\alpha_{i_o 1},\ldots,\alpha_{i_o n_{i_o}})$ appartient à A.

(**Déf.5**) Un ensemble $A \subseteq T$ est dit fermé M-recursif ssi:

1) $\{a_1,\ldots,a_n\} \subseteq A$.

2) A est fermé par rapport aux opérations $f_1,\ldots,f_s$.

Avec ces définitions, les théorèmes précédents deviennent:

Théorème 2': L'ensemble M est le plus petit ensemble fermé M-récursif.

Théorème 3': M est l'intersection de tous ensembles fermés M-récursifs.

(**Déf,6**) Le système d'éléments $\langle \alpha_1,\ldots,\alpha_m \rangle$, $m \geq 1$ et

$\alpha_i \in T$ pour $i \in \{1,2,\ldots,m\}$, constitue une description M-récursive pour l' élément α, si $\alpha_m = \alpha$ et que chaque α_i ($i \in \{1,2,\ldots,m\}$) satisfait au moins l'une des propriétés:

1) $\alpha_i \in \{a_1,\ldots,a_n\}$.
2) α_i s'obtient à partir ds éléments qui le précedent dans le système en appliquant les fonctions f_j, $1 \le j \le s$ definies par la proprieté 2^o de (déf.1).

(Déf.7) Le nombre m de ce système s'appelle la longueur de la description M-récursive pour l'élément α.

Observation 3: Si l'élément α admet une description M-récursive, alors il admet une infinité de telles descriptions.

En effet, si $\langle \alpha_1,\ldots,\alpha_m \rangle$ est une description M-récursive de α alors $\langle \underbrace{a_1,\ldots,a_1}_{\text{h fois}}, \alpha_1,\ldots,\alpha_m \rangle$ est aussi une description M-récursive pour α, h pouvant prendre toute valeur de N.

Théorème 4: L'ensemble M est confondu avec l'ensemble de tous les éléments de T qui admettent une description M-récursive.

Preuve: soit D l'ensemble de tous éléments qui admettent une description M-récursive. Nous allons démontrer par récurrence que $M_p \subseteq D$ pour tout p de $\mathbf{N}^*$.

Pour $p = 1$ on a: $M_1 = \{a_1,\ldots,a_n\}$, et les a_j, $1 \le j \le n$ admettent comme descrition M-récursive: $<a_j>$. Ainsi $M_1 \subseteq D$ Supposons que la propriété est vraie pour les valeurs inférieures à p. M_p est obtenu en appliquant la règle 2^o aux éléments de

$\bigcup_{i=1}^{p-1} M_i$; $\alpha \in M_p$ entraine $\alpha \in f_j(\alpha_{i_1},...,\alpha_{i_{n_i}})$ et $\alpha_{i_j} \in M_{hj}$ pour $h_j < p$ et $1 \le j \le n_i$.

Mais α_{i_j}, $1 \le j \le n_i$, admet des descriptions M-récursives d'après l'hypothèse de récurrence, soit $\langle \beta_{j1},...,\beta_{js_j} \rangle$. Alors $\langle \beta_{11},...,\beta_{1s_1},\beta_{21},...,\beta_{2s_2},...,\beta_{n_i1},...,\beta_{n_is_{n_i}},\alpha \rangle$ constitue une description M-récursive pour l'élément α. Donc si α appartient à D, alors $M_p \subseteq D$ càd $M = \bigcup_{p \in \mathbb{N}^*} M_p \subseteq D$.

Réciproquement, soit x appartenant à D. Il admet une description M-récursive $\langle b_1,...,b_t \rangle$ avec $b_t = x$. Il en résulte par récurrence sur la longueur de la description M-récursive de l'élément x, que $x \in M$. Pour $t = 1$, on a $\langle b_1 \rangle$, $b_1 = x$ et $b_1 \in \{a_1,...,a_n\} \subseteq M$. On suppose que tous les éléments y de D qui admettent une descrition M-récursive de longueur inférieure à t appartiennent à M. Soit $x \in D$ décrit par un système de longueur t: $\langle b_1,...,b_t \rangle$, $b_t = x$. Alors $x \in \{a_1,...,a_n\} \subseteq M$, cu bien x est obtenu en appliquant la règle 2° aux éléments qui le précèdent dans le système : $b_1,..., b_{t-1}$.
Mais ces éléments admettent des descriptions M-récursives de longueurs inférieures à t: $\langle b_1 \rangle$, $\langle b_1, b_2 \rangle,...,\langle b_1,...,b_{t-1} \rangle$. D'après l'hypothèse de récurrence, $b_1,..., b_{t-1}$ appartiennent à M.
Donc b_t appartient aussi à M. Il en résulte que $M \equiv D$.

Théorème 5: Soient $b_1,...,b_q$ des éléments de T qui s'obtiennent à partir des éléments $a_1,...,a_n$ en appliquant un nombre fini de fois les opérations $f_1, f_2,...,$ ou f_s. Alors M

peut être défini récursivement de la façon suivante:

1) Certains éléments $a_1,\dots,a_n$, $b_1,\dots,b_q$ de T appartiennent à M.

2) M est fermé pour les applications f_i, avec $i \in \{1,2,\dots,s\}$.

3) Chaque élément de M est obtenu en appliquant un nombre fini de fois les règles (1) ou (2) qui précèdent.

Prouve: évidente. Comme $b_1,\dots,b_q$ appartiennent à T, et s'obtiennent à partir des éléments $a_1,\dots,a_n$ de M en appliquant un nombre fini de fois les opérations f_i, il en résulte que $b_1,\dots,b_q$ appartiennent à M.

Théorème 6: Soient g_j, $1 \le j \le r$, des opérations n_j–aires, càd $g_j : T^{n_j} \to T$ telles que M soit fermé par rapport à ces opérations. Alors M peut être defini récursivement de la façon suivante:

1) Certains éléments $a_1,\dots,a_n$ de T appartiennent à M.

2) M est fermé pour les opération f_i, $i \in \{1,2,\dots,s\}$ et g_j, $j \in \{1,2,\dots,r\}$.

3) Chauqe élément de M est obtenu en appliquant un nombre fini de fois les règles précédentes.

Preuve facile: comme M est fermé pour les opérations g_j (avec $j \in \{1,2,\dots,r\}$), on a, quels que soient $\alpha_{j1},\dots,\alpha_{jn_j}$ de M, $g_j(\alpha_{j1},\dots,\alpha_{jn_j}) \in M$ pour tout $j \in \{1,2,\dots,r\}$.

Les théorèms 5 et 6 entraînent:

Théorème 7: L'ensemble M peut être défini récursivement de la façon suivante:

1)Certains éléments $a_1,\dots,a_n$, $b_1,\dots,b_q$ de T appartiennent à M.

2) M est fermé pour les opérations f_i $(i \in \{1,2,\dots,s\})$ et pour les opérations g_j $(j \in \{1,2,\dots,r\})$ définies précédemment.
3) Chaque élément de M est défini en appliquant un nombre fini de fois les 2 règles précédentes.

Déf.8) L'operation f_i conserve la propriété P ssi quels que soient les élements $\alpha_{i1},\dots,\alpha_{in_i}$ ayant la propriété P, $f_i(\alpha_{i1},\dots,\alpha_{in_i})$ a la propriété P.

Théorème 8: Si $a_1,\dots,a_n$ ont la propriété P, et si les fonctions $f_1,\dots,f_s$ consevent cette propriété, alors tous les éléments de M ont la propriété P.

Preuve:

$M = \bigcup_{p \in N^*} M_p$. Les élémente de M_1 ont la propriété P.

Supposons que les elements de M_i pour $i < p$ ont la propriété P. Alors les éléments do M_p l'ont aussi parce que M_p s'obtient en appliquant les opérations $f_1,\dots,f_s$ aux éléments de: $\bigcup_{i=1} M_i$, éléments qui ont propriété P. Donc, quel que qoit p de N, les éléments de M_p ont la propiété P.

Donc tous les éléments de M l'ont.

Conséquence 1: Soit la propriété P: "x peut être represente sous la forme $F(x)$".

Si $a_1,\dots,a_n$ peuvent être représentés sous la forme $F(a_1)$,..., respectivement $F(a_n)$, et si $f_1,\dots,f_s$ conservent la propriété P, alors tout élément α de M peut etre resprésenté sous la forme $F(\alpha)$.

Rem. on peut trouver encore d'autres déf. equivalentes de M.

2 - APPLICATIONS, EXEMPLES.

Dans les applications, certaines notions générales comme: élément M-récursif, description M-récursive, ensemble fermé M-récursif seront remplacés par les attributs caracterisant l'ensemble M. Par exemple dans la théorie des fonctions récursives, on trouve des notions comme: fonctions primitives récursives, description primitive récursive, ensemble fermé primitivement récursif. Dans ce cas "M" a été remplacé par l'attribut "primitif" qui caracterise cette classe de fonctions, mais il peut etre remplacé par les attributs "général", "partiel".

En particularisant les régles 1° et 2° de la déf.1, on obtient plusieurs ensembles intéressants:

Exemple 1: (voir [2], pages 120-122, problème 7.97).

Exemple 2: L'ensemble des termes d'une suite définie par une relation de récurrence constitue un ensemble récursif.

Soit la suite: $a_{n+k} = f(a_n, a_{n+1}, \ldots, a_{n+k-1})$ pour tout n de $\mathbf{N}^*$, avec $a_i = a_i^o$, $1 \le i \le k$. On va construire récursivement l'ensemble $A = \{a_m\}_{m \in \mathbf{N}^*}$ et on va définir en même temps la position d'un élément dans l'ensemble A:

1°) $a_1^o, \ldots, a_k^o$ appartiennent à A, et chaque a_i^o $(1 \le i \le k)$ occupe la position i dans l'ensemble A;

2°) si $a_n, a_{n+1}, \ldots, a_{n+k-1}$ appartiennent à A, et chaque a_j pour $n \le j \le n+k-1$ occupe la position j dans l'ensemble A, alors $f(a_n, a_{n+1}, \ldots, a_{n+k-1})$ appartient à A et occupe la position $n + k$ dans l'ensemble A.

3°) chaque élément de B s'obtient en appliquant un nombre fini de fois les règlea 1° ou 2°.

Exemple 3: Soit $G = \{e, a^1, a^2, \ldots, a^p\}$ un groupe cyclique

engendré par l'element a. Alors (G, •) peut être defini récursivement de la facon suivante:

1°) a appartient à G.

2°) si b et c appartiennent à G alors $b \cdot c$ appartiennent à G.

3°) chaque élément de G est obtenu en appliquant un nombre fini de fois les règles 1 ou 2.

Exemple 4: Chaque ensemble fini $ML = \{x_1, x_2, \dots, x_n\}$ peut être défini récursivement (avec $ML \subseteq T$):

1°) Les éléments $x_1, \dots, x_n$ de T appartiennent à ML.

2°) Si a appartient à ML, alors $f(a)$ appartient à ML, où $f: T \rightarrow T$ telle que $f(x) = x$;

3°) Chaque élément de ML est obtenu en appliquant un nombre fini de fois les règles 1° ou 2°.

Exemple 5: Soit L un espace vectoriel sur le corps commutatif K et $\{x_1, \dots, x_m\}$ une base de L. Alors L être défini récursivement de la façon suivante:

1°) $x_1, \dots, x_m$ appartiennent à L;

2°) si x, y appartiennent à L et si a appartient à K, alors $x \perp y$ y appartient à L et a $a * x$ appartient à L;

3°) chaque élément de L est obtenu récursivement en appliquant un nombre fini de fois les règles 1° ou 2°.

(Les lois $\perp$ et $*$ sont respectivement les lois interne et externe de l'espace vectoriel L).

Exemple 6: Soient X un A-module, et $M \subset X$ $(M \neq \varnothing)$, avec $M = \{x_i\}_{i \in I}$ Le sous-module engendré par M est:

$$\langle M \rangle = \{x \in X \mid x = a_1 x_1 + \dots + a_n x_n, a_i \in A, x_i \in M, i \in \{1, \dots, n\}\}$$

peut être défini recursivement de la façon suivante:

1°) pour tout i de $\{1,2,\dots,n\}, \{1,2,\dots,n\}$. $x_i \in \langle M \rangle$;

2°) si x et y appartiennent à $<M>$ et a appartient à A, alors $x+y$ appartient à $<M>$, et ax aussi;

3°) chaque élément de $<M>$ est obtenu en appliquant un nombre fini de fois les regles 1° ou 2°.

En accord avec le paragraphe 1 de cet article, $<M>$ est le plus petit sous-ensemble de X verifiant les condition 1° et 2°, c'est-à-dire que $<M>$ est le plus petit sous-module de X incluant M. $<M>$ est aussi l'intersection de tous les sous-ensembles de X vérifiant les conditions 1° et 2°, c'est-à-dire que $<M>$ est l'intersection de tous les sous-modules de X qui contiennent M. On retrouve ainsi directement quelques résultats classiques d'algèbre.

On peut aussi parler de sous-groupes ou d'idéal engendré par un ensemble: on obtient ainsi quelques applications importantes en algèbre.

Exemple 7: On obtient aussi comme application la théorie des langages formels, parce que, comme on le sait, chaque langage régulier (linéaire à droite) est un ensemble régulier et réciproquement. Mais un ensemble régulier sur un alphabet $\sum=\{a_1,\dots,a_n\}$ peut être défini récursivement de la façon suivante:

1°) $\varnothing,\{\varepsilon\},\{a_1\},\dots,\{a_n\}$ appartiennent à R.

2°) si P et Q appartiennent à R, alors $P\cup Q$, PQ, et P^* app. à R, avec $P\cup Q=\{x \,/\, x\in P \text{ ou } x\in Q\}$; $PQ=\{xy \,/\, x\in P \text{ et } y\in Q\}$, et $P^*=\bigcup_{n=0}^{\infty}P^n$ avec $P^n=\underbrace{P\cdot P\dots P}_{n \text{ fois}}$ et, par convention, $P^0=\{\varepsilon\}$.

3°) Rien d'autre n'appartient à R que ce qui est obtenu à l'aide de 1° ou de 2°.

D'ou plusieurs propriétés de cette classe de langages avec applications aux langages de programmation.

Bibligraphie:

[1] C.P.Popovici, L.Livovschi, H.Georgescu, N.Ţăndăreanu - "Curs de bazele informaticii (funcţii booleene şi circuite combinaţionale)" Tipografia Universităţii din Bucarest, 1976.

[2] F.Smarandache -"Problemes avec et sens...probemes!" - Somipress, Fès (Maroc), 1983.

A GENERALIZATION IN SPACE OF JUNG'S THEOREM

In this short note we will prove a generalization of joung's theorem in space.

Theorem. Let n be points in space such that the maximum distance between two ones be a. Prove that exists a sphere of radius $r \le a\frac{\sqrt{6}}{4}$ which contains in interior or on surface all these points.

Proof:

Let the points $P_1,\ldots,P_n$. Let there be a sphere $S_1(O_1,r_1)$ of center O_1 and radius r_1 which contains all these points. We note $r_2 = \max\limits_{1\le i\le n} P_iO_1 = P_1O_1$ and construct the sphere $S_2(O_1,r_2)$, $r_2 \le r_1$, with $P_1 \in Fr(S_2)$ where $Fr(S_2)$ = frontier (surface) of S_2.

We apply a homothety H in space, of center P_1, such that the new sphere $H(S_2) = S_3(O_3,r_3)$ has the property: $Fr(S_3)$ contains another point, for example P_2, and of course S_3 contains all points P_i.

1) If P_1, P_2 are diametricalli opposite in S_3 then $r_{\min} = \frac{a}{2}$.

If no, we do a rotation R so that $R(S_3) = S_4(O_4,r_4)$ for which $\{P_3,P_2,P_1\} \subset Fr(S_4)$ and S_4 contains all points P_i.

2) If $\{P_1,P_2,P_3\}$ belong to a great circle of S_4 and they are not included in an open semicircle, then $r_{\min} \le \frac{a}{\sqrt{3}}$ (Jung's theorem).

If no, we consider the fascicule of spheres S for which $\{P_1, P_2, P_3\} \subset Fr(S)$ and S contains all points P_i. We choose a sphere S_5 such that $\{P_1, P_2, P_3, P_4\} \subset Fr(S_5)$.

3) If $\{P_1, P_2, P_3, P_4\}$ are not included in an open semisphere of S_5 then the tetrahedron $\{P_1, P_2, P_3, P_4\}$ can be included in a regulated tetrahedron of side a, whence we find the radius of S_5 is $\leq a\frac{\sqrt{6}}{4}$.

If no, let's $\max\limits_{1 \leq i \leq j \leq 4} P_i P_j = P_1 P_4$. Does the sphere S_6 of diameter $P_1 P_4$ contain all points P_i?

If yes, stop (we are in the case 1).

If no, we consider the fascule of spheres S' such that $\{P_1, P_4\} \subset Fr(S')$ and S' contains all points P_i. We choose another sphere S_7 for which $P_5 \notin \{P_1, P_2, P_3, P_4\}$ and $P_5 \in Fr(S_7)$.

With these new notations (the points P_1, P_4, P_5 and the sphere S_7) we return to the case 2.

This algorithm is fonite; it constructs the asked sphere.

[Published in "GAZETA MATEMATICĂ", Nr. 9-10-11-12, 1992, Bucharest, Romania, p.352.]

MATHEMATICAL RESEARCH AND NATIONAL EDUCATION

In our days focus strongly on the interrelation between research and production. Between these two fields there is actually a very tight relation (osmosis), a dialectical union, while each is maintaining its own personality.

Education has develop according to its needs and exigencies resulting from the technical and scientific revolution: The introduction of faculties in the fields of production, research and design areas, and vice versa, the necessity of introducing the process of production and research work in the school units.

Therefore, it should be kept in mind, that the disertation projects of the students be immediately used in the process of production.In this case, it falls to the school the resposibility to repare and shape the future specialists in all fields of activity.

In the light of the present reality, we are witness to an informational burst in all domains, and it is noticed the sustained effort which is being made by the educational system to adopt itself to the over increasing exigencis of the society, to keep in pace with the technique and science conquests. Within these science conquests, mathematics occupies a central place -"the queen of sciences", as Gauss has said.

The Mathematics, for the ones who are studying it, confess them, by the precision of formule and expressions on epoch, there have developed much, so that transforming it from a science of number and of quantities (as it was called in ancient times) in a science of essential structures. New branches of mathematics have appeared, many of them thanks to its

interpenetration with other sciences, and even branches such as: Mathematical Linguistics, Mathematical Poetics (in the latter a remarkable contribution being due to Prof. Solomon Marcus from Bucharest University). (The Mathematical Linguistics having as a starting point the topic models of the natural language and developing on algebraic grammar, by which are being sudied the phenomenons of the natural languages).

"(...) mathematics has no limits, and the space that it finds is, so far, too reduced for its aspirations. The possibilities in Mathematics are as unlimited as the ones of the worlds which ceaselessly grow and multiply under the scrutinizing gaze of the astronomers; the mathematics could not be reduced by limited, precise keys or to be reduced to valid definitions eternally, but as the conscience life, which seem dormant in every world, each stone, each leaf, each bloom of flower, and in each which it is permanently ready to burst in new forms of animal life and vegetal existance" (James - Joseoh Sylvester, English Mathematician).

Mathematics in other sciences.

We say that it iz about their mathematization. All these sciences could not progress if they were not mathematized. Therefore, a whole group of discoveries wouldn't have taken place had it not been for the knowledge of certain scientifical procedures, if mathematics had not possessed a certain quantity of knowledge (i.e., Einstein hadn't discovered the theory of relativity and if before him the Tensorial Calculator had not been discovered).Although other discoveries have been made before using math's calculations, which afterwards experimentally have been proved (Physician Maxwell - has generalized the concept of the field of electromagnetic forces, underlining the fact that even reforming to an electric or

magnetic field this is propulgated in existence by waves with the light speed.)

Mathematics also offers its possibilities to the technical field, solving problems arising in the production process.

The very high abstractness in Mathematics does not hinder under its immediate applicability in practical manner, such would be worth while mentioning a few examples:

- The Roumanian geometer Gh.Ţiţeica made discoveries in the field of differential geometry - which led twenty years later to the conclusion that these could be applied in the theory of generalized relativity;

- Cayley has discovered the matrix, discovery which found its applicability eighty seven years later when Heisenberg used it in the quantic mechanics;

- The English Mathematician George Boole, by the middle of XIXth century, discovered the algebra which carries his name and which occupies the worthy place in the software - electronic computers.

An interesting correlation existe between mathematics and arts: music, painting sculpture, architecture, and poetry.

Art is the pure expression of the "sentiment" while Mathematics is the crystalline expression of the pure "reasoning". Art, gushing from a sentiment, is warmer and more human, while mathematics, springing out from reasoning, is colder, but glitters more. An interesting correlation between Arts (and Literature especially), has been made by Solomon

Marcus, Professor in the Depatments Of Mathematics and of Languages also, showing the superiority of the pure artistic language vis-a-vis of the scientific language.

While the scientific language has a unique sense, the literary one has an infinite. Therefore, in science the ambiguous language is eliminated. Recalling "this luminous point where geometry meets the poetry" as the mathematician and poet Dan Barbilian was saying, and we are reminded also the following idea:

"The poem of the future, by excellence, the sublime poem, will be borrowed from science" (Piere - Jules - César Jensen).

Generally speaking about research, the risks that the scientist might run should be mentioned:

- he may find results already known (but this shouldn't represent a disillusion, but even satifaction);
- there cold be a lead to suggestive results (one should have patience, and persevere);
- one could have errors in his demonstrations (deductions) - (almost all mathematicians have committed errors).

JUBILEE OF "GAMMA" MAGAZINE

This autumn will be a few years since the school magazine "Gamma" was founded at Liceul "Steagu Roșu" in Brașov, Romania, under the guidance of the good hearted professor MIHAIL BENCZE, who has not spared any effort for it.

In the 28 numbers issued up to present, "Gamma" magazine has encouraged in solving problems of mathematics of over two thousand students, helping them prepare for scientific competitons, exams grades and degrees for universities. Each year, the Editorial office grants prizes and honorable mentions to the most hardworking pupils who solve problems.

The magazine structure is classic. The wider space is dedicated to the original proposed problems of mathematics for grades 8 - 12 and university levels of comuter science, up the present exceeding 7ooo, out of which we are sure that any time branch of very interesting problems, highly difficult can be selected. We recall that some of those have already appeared in prestigious foreign magazines - i.e., " American Mathematical Monthly". "Mathematics Magazine", etc. We also recall the over 8o **open problems**, among which some may constitute topics of research for the mathematicians of tomorrow. Some elegant and ingenious problems are solved/resolved in the pages of this magazine. The journal also contains problems translated from foreign magazines ("Kvant", A.M.M.) or foreign collections, problems given at olympiads of mathematics from other countries (Spain, Belgium, Tunisia, Morocco, etc.) as well as from our country (GMB, RMT, Matematikai Lapok) some with solutions or even with generalizations of problems from the magazines mentioned above.

Also, over one hundred "Where is the fault? (in demonstrations)" notes of mathematics.

There have been over 130 papers for vulgarization of mathematics or matters concerning inter disciplinarity, mathematics and other domains (physics, phylosophy, psychology, etc.) or even of creation.

The column "Mini Mathematical History", sustained regularity by Prof. M. Bencze, schematically presented approximately 150 Roumanian and foreign biographies of mathematicians.

Among the collaborators included for the magazine (other than the students, who are the most numerous for in fact it is their magazine) are professors, engineers, computer science specialists, and university faculty. Many are recognized in their field of specialty.

The foreign collaborators (Dr.E.Grosswald, Dr.Leroy F. Meyers (U.S.A.), Prof. Francisco Bellot (Spain), are famous in the world of Mathematics. Additionally, the Editorial office sporadically published Mathematical paradoxes, cross words, "Mathematical Poems", and columns (such as"... did you know that.."), graphic themes and mottos (let us better call them, words of wisdom) of famous people.

It remains Long Live Mathematics.

September 1987

[Published in "Gamma", XXIX-XXX, Anul X, No. 1-2, October 1987 pp. 7-8.]

LA MULȚI ANI ÎN MATEMATICI!

Prin bunăvoința profesorului Gane Policarp am intrat în posesia mai multor numere din ”Caietul de informare matematică, alcătuit cu migală și pricepere, care m-a atras și îndemnat de la început să colaborez cu mici materiale.

Preocuparea redactorilor pentru prezentarea problemelor date la concursuri și olimpiade școlare, la examene de treaptă, bacalaureate m-a determinat să-i acord un loc de cinste în modesta mea bibliotecă, și să lucrez cu elevi de-ai mei probleme propuse aici, unii dintre ei înscrindu-și numele la rubrica rezolvitorilor.

Acum aflu cu o surprindere plăcută că revista matematicienilor câmpineni împlinește 1o ani de existență neântreruptă.

Drum lung și în continuare!

(Ianuarie 1988)

DEDUCIBILITY THEOREMS IN MATHEMATICS LOGIC

SUMMARY

In this paper I shall give two own theorems from the Propositional Calclus of the "Mathematics Logic" with their consequences and applications.

§ 1. THEOREMS,CONSEQUENCES

In the begining I shall put forward the axioms of the Propositional Calculus.

I. a) $\vdash A \supset (B \supset A)$,

b) $\vdash (A \supset (B \supset C)) \supset ((A \supset B) \supset (A \supset C))$.

II. a) $\vdash A \wedge B \supset A$,

b) $\vdash A \wedge B \supset B$,

c) $\vdash (A \supset B) \supset ((A \supset C) \supset (A \supset B \wedge C))$.

III. a) $\vdash A \supset A \vee B$,

b) $\vdash B \supset A \vee B$,

c) $\vdash (A \supset C) \supset ((B \supset C) \supset (A \vee B \supset C))$.

IV. a) $\vdash (A \supset B) \supset (\overline{B} \supset \overline{A})$,

b) $\vdash A \supset \overline{\overline{A}}$.

c) $\vdash \overline{\overline{A}} \supset A$

THEOREM. If: $\vdash A_i \supset B_i$, $i = \overline{1,n}$, then

1) $\vdash A_1 \wedge A_2 \wedge \ldots \wedge A_n \supset B_1 \wedge B_2 \wedge \ldots \wedge B_n$,

2) $\vdash A_1 \vee A_2 \vee \ldots \vee A_n \supset B_1 \vee B_2 \vee \ldots \vee B_n$.

Proof:

It is made by complete induction. For $n = 1$: $\vdash A_1 \supset B_1$, let's show that $\vdash A_1 \supset B_1$ (obiously). For $n = 2$: hypothesis $\vdash A_1 \supset B_1$, $\vdash A_2 \supset B_2$; les's show that $\vdash A_1 \wedge A_2 \supset \supset B_1 \wedge B_2$. We use the axiom II, c) replacing $A \to A_1 \wedge A_2$, $B \to B_1$, $C \to B_2$ it results:

(1) $\vdash (A_1 \wedge A_2 \supset B_1) \supset ((A_1 \wedge A_2 \supset B_2) \supset \supset (A_1 \wedge A_2 \supset B_1 \wedge B_2))$.

We use the axiom II, a) replacing $A \to A_1$, $B \to A_2$; we have $\vdash A_1 \wedge A_2 \supset A_1$. But $\vdash A_1 \supset B_1$ (hypothesis) applying the syllogism rule, it result $\vdash A_1 \wedge A_2 \supset B_1$. Analogously, using the axiom II, b), we have $\vdash A_1 \wedge A_2 \supset B_2$. We know that $\vdash A_1 \wedge A_2 \supset B_i$, $i = 1,2$, are deducible, then applying in (I) inference rule twice, we have $\vdash A_1 \wedge A_2 \supset B_1 \wedge B_2$.

We suppose it's true for n; let's prove that for $n + 1$ it is true. In $\vdash A_1 \wedge A_2 \supset B_1 \wedge B_2$ replacing $A_1 \to A_1 \wedge \ldots \wedge A_n$, $A_2 \to A_{n+1}$, $B_1 \to B_1 \wedge \ldots \wedge B_n$, $B_2 \to B_{n+1}$ and using induction hypothesis it results $\vdash A_1 \wedge \ldots \wedge A_n \wedge A_{n+1} \supset B_1 \wedge \ldots \wedge B_n \wedge B_{n+1}$ and item 1) from the Theorem is proved.

2) It is made by induction. For $n = 1$; if $\vdash A_1 \supset B_1$, then $\vdash A_1 \supset B_1$. For $n = 2$: if $\vdash A_1 \supset B_1$ and $\vdash A_2 \supset B_2$, then $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$.

We use axiom III, c) replacing $A \to A_1$, $B \to A_2$, $C \to B_1 \vee B_2$ we get

$$(2) \quad \vdash (A_1 \supset B_1 \vee B_2) \supset ((A_2 \supset B_1 \vee B_2) \supset \supset (A_1 \vee A_2 \supset B_1 \vee B_2)).$$

Let's show that $\vdash A_1 \supset B_1 \vee B_2$. We use the axiom III, a) replacing $A \to B_1$, $B \to B_2$ we get $\vdash B_1 \supset B_1 \vee B_2$ and we know from the hypothesis $A_1 \quad B_1$. Applyind the syllogism we get: $\vdash A_1 \supset B_1 \vee B_2$.

In the axiom III, b) replacing $A \to B_1$, $B \to B_2$, we get $\vdash B_2 \supset B_1 \vee B_2$. But $\vdash A_2 \supset B_2$ (from the hypothesis, applying the syllogism we get $\vdash A_2 \supset B_1 \vee B_2$. Applying the inference rule twice in (2) we get $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$.

Suppose it's true n and let's show that for $n + 1$ it is true. Replace in $\vdash A_1 \vee A_2 \supset B_1 \vee B_2$ (true formula if $\vdash A_1 \supset B_1$ and $\vdash A_2 \supset B_2$) $A_1 + A_1 \vee \ldots \vee A_n$, $A_n + A_{n+1}$, $B_1 \to B_1 \vee \ldots \vee B_n$, $B_2 \to B_{n+1}$. From induction hypothesis it results $\vdash A_1 \vee \ldots \vee A_n \vee A_{n+1} \supset B_1 \vee \ldots \vee B_n \vee B_{n+1}$ and the Theorem is proved.

CONSEQUENCES

1° If $\vdash A_i \supset B$, $i=\overline{1,n}$, then $\vdash A_1 \wedge \ldots \wedge A_n \supset B$.

2° If $\vdash A_i \supset B$, $i=\overline{1,n}$, then $\vdash A_1 \vee \ldots \vee A_n \supset B$.

Proof: 1°) Using 1) from the Theorem, we get

3) $\vdash A_1 \wedge \ldots \wedge A_n \supset B \wedge \ldots \wedge B$ (n times).

In axiom II, a) we replace $A \to B$, $B \to B \wedge \ldots \wedge B$ ($n-1$ times), we get

(4) $\vdash B \wedge \ldots \wedge B \supset B$ (n times)

From (3) and (4) by means of the syllogism rule we get

$\vdash A_1 \wedge \ldots \wedge A_n \supset B$.

2°) Using 2) from Theorem, we get

$\vdash A_1 \vee \ldots \vee A_n \supset B \vee \ldots \vee B$ (n times).

LEMMA. $\vdash B \vee \ldots \vee B \supset B$ (n times), $n \geq 1$.

Proof:

It is made by induction. For $n = 1$, obvioully. For $n = 2$: in axiomIII, c) we replace $A \to B$, $C \to B$ and we get

$\vdash (B \supset B) \supset ((B \supset B) \supset (B \vee B \supset B))$. Applying the inference rule twice we get $\vdash B \vee B \supset B$.

Suppose for n that the formula is deducible, let's prove that is for $n+1$.

We proved that $\vdash B \supset B$. In axiom III, c) we replace $A \to B \vee \ldots \vee B$ (n times), $C \to B$, and we get $\vdash (B \vee \ldots \vee B \supset B) \supset ((B \supset B) \supset (B \vee \ldots \vee B \supset B))$ (n times). Applying two

times the inference rule, we get $\vdash B\vee\ldots\vee B\supset B(n+1 \text{ times})$ so Lemma is proved.

From $\vdash A_1\vee\ldots\vee A_n\supset B\vee\ldots\vee B$ (n times) and applying the syllogism rule, from Lemma we get $\vdash A_1\vee\ldots\vee A_n\supset B$.

3°) $\vdash A\wedge\ldots\wedge A\supset A$ (n times)

4°) $\vdash A\vee\ldots\vee A\supset A$ (n times).

Previously we proved, replacing in Consequences 1°) and 2°), $B\rightarrow A$. Analogously, the consequences are proven:

5°) If $\vdash A\supset B_i$, $i=\overline{1,n}$, then $\vdash A\supset B_1\wedge\ldots\wedge B_n$.

6°) If $\vdash A\supset B_i$, $i=\overline{1,n}$, then $\vdash A\supset B_1\vee\ldots\vee B_n$.

Analogously,

7°) $\vdash A\supset A\wedge\ldots\wedge A$ (n times)

8°) $\vdash A\supset A\vee\ldots\vee A$ (n times)

9°) $\vdash A_1\wedge\ldots\wedge A_n\supset A_1\vee\ldots\vee A_n$.

Proof:

The method I. It is initially proved by induction: $\vdash A_1\wedge\ldots\wedge A_n\supset A_i$, $i=\overline{1,n}$ and 2) is applied from the Theorem.

The method II. It is proven by iduction that: $\vdash A_i\supset A_1\wedge\ldots\wedge A_n$, $i=\overline{1,n}$ and then 1) is applied from the Theorem.

10°) If $\vdash A_i\supset B_i$, $i=\overline{1,n}$, then $\vdash A_1\wedge\ldots\wedge A_n\supset$
$\supset B_1\vee\ldots\vee B_n$

Proof:

Method I. Using 1) from the Theorem, it results:

(5) $\vdash A_1 \wedge \ldots \wedge A_n \supset B_1 \wedge \ldots \wedge B_n$

We apply the Conseq. 9^o) Where we replace $A_i \to B_i$, $i = \overline{1,n}$ and results:

(6) $\vdash B_1 \wedge \ldots \wedge B_n \supset B_1 \vee \ldots \vee B_n$.

From (5) and (6), applying the syllogism rule we get 10^o).

Method II. We firstly use the Conseq, 9^o) and then 2) from the Theorem and so we the Conseq. 10^o).

§ 2. APPLICATIONS AND REMARKS ON THEOREMS

The theorems are used in order to prove the formulae of the shape:

$$\vdash A_1 \wedge \ldots \wedge A_p \supset B_1 \wedge \ldots \wedge B_r$$

$$\vdash A_1 \vee \ldots \vee A_p \supset B_1 \vee \ldots \vee B_r, \text{ where } p,r \in \mathbb{N}^*$$

It is proven that $\vdash A_i \supset B_j$, i.e.

$$\forall i \in \overline{1,p},\ \exists j_o \in \overline{1,r},\ j_o = j_o(i),\quad \vdash A_i \supset B_{j_o}$$

and

$$\forall j \in \overline{1,r},\ \exists i_o \in \overline{1,p},\ i_o = i_o(j),\quad \vdash A_{i_o} \supset B_j.$$

EXEMPLES. The following formulae are deducible:

(i) $\vdash A \supset (A \vee B) \wedge (B \supset A)$,

(ii) $\vdash (A \wedge B) \vee C \supset A \vee B \vee C$,

(iii) $\vdash A \wedge C \supset A \vee C$

Solution:

(i) We have $\vdash A \supset A \vee B$ and $\vdash A \supset (B \supset A)$ (axiom III, a) and I, a)) and according 1) from Theorem it results (i).

(ii) From $\vdash A \supset (B \supset A)$, $\vdash A \wedge B \supset B$, $\vdash C \supset C$ and Theorem 1), we have (ii).

(iii) Method I. From $\vdash A \wedge C \supset A$, $\vdash A \wedge C \supset C$ and Theorem 2), Method II. From $\vdash A \supset A \vee C$, $\vdash C \supset A \vee C$ and using Theorem 1).

REMARKS. 1) The reciprocals of Theorem 1) and 2) are not always true.

a) Antiexample for Theorem 1). The formula $\vdash A \wedge B \supset \supset A \wedge A$ is deducible from axiom II, a), $\vdash A \wedge A \supset A$ (Conseq. 7^{0}) and syllogism rule. But $\vdash A \supset A$ for all, that the formula $B \supset A$ is not deducible, so the reciprocal of the Theorem 1) is false.

Antiexemple for Theorem 2). The formula $\vdash A \vee A \supset \supset A \vee B$ is deducible from Lemma, axiom III, a) and applying the syllogism rule. But $\vdash A \supset A$ for all, that the formula $A \supset B$ is not deducible, so the reciprocal of Theorem 2) is false.

2) The contraries of Theorem 1) and 2) are not always true. Antiexemples:

a) for Theorem 1): $\vdash A \supset A$ and $B \not\supset A$ results that $\vdash A \wedge B \supset A \wedge A$ so the contrary of Theorem 1) is false:

b) for Theorem 2): $\vdash A \supset A$ and $A \not\supset B$ results that

$\vdash A \vee A \supset A \vee B$ so te contrary of Theorem 2) is false.

BIBLIOGRAPHY

[1] P.S. NOVIKOV, Elemente de logică matematică, Editura Ştiinţifică, Bucureşti, 1966.

[2] H.FREUDENTHAL, Limbajul logicii matematice, Editura Tehnică, Bucureşti, 1973.

UNIVESITATEA DIN CRAIOVA 24.10.1979
Facultatea de Ştiinţe Exacte

[Published in "An.Univ. Timişoara", seria Şt. matematice, Vol.XVII, fasc. 2, 1979, pp. 164-8.]

LINGUISTIC - MATHEMATICAL STATISTICS IN RECENT ROMANIAN POETRY

"Mathematics is logical enough to be able to detect the internal logics of poetry and "crazy enough not to lag behind the poetic ineffable" (Solomon Marcus).

The author of this article aims a statistic investigation of a recently publishel volume of poetry [3] which will make possible some more general conclusions on the evolution of poetry in the XX-th century (be the literary current hermetism, surrealism or any other). Certain modifications in the structure of poetry occurred in its evolution from classicism to modernism are also presented. Men of letters have never agreed with mathematics and, especially, with its interference in art. Let us quote one of them: "Remarquez que, a mon avis, tout littérature est grotesque ... (...) La seule excuse de l'ecrivain c'est de se rendre compte qu'iljoue, que la litterature est un jeu" (Eugène Ionesco). Well, if literature is a game why could not be subjected to nathematical investigation?

The book chosen for this study (see [3]) contains 44 poems (for which the frist and the last are sort of poem essays on Romanian poetry). It comprises over 25o sentences, over 7oo verces, over 2,5oo words and over 11,7oo letters (not sounds).

MORPHOLOGICAL ASPECTS

1. The frequency of words depending on the gramatical category they belong to.

1. Nouns	35.592%	"empty words 40.271%
2. Verbo (predicat. moods)	13.o79%	
3. Adjectives	6.183%	
4. Adverbs	4.829%	
"Full" words	59.729%	

2. The average distribution of "full" words[1] per verses (lines), sentences, poems

a) 1.255	nouns/line
b) o.461	verbs (p.m)/line
c) o.218	adjectives/line
d) o.172	adverbs/line
e) 3.464	nouns/sentence
f) 1.273	verbs (p.m)/sentence
g) o.6o2	adjectives/sentence
h) o.475	advers/sentence
i) 2o.393	nouns/poem
j) 7.492	verbs (p.m)/poem
k) 3.543	adjectives/poem
l) 2.795	adverbs/poem

We may conclude:

CONJECTURE 1. In the recent Romanian poetry the percentage of adjectives is, on an average, under is of the total of words.

CONJECTURE 2. The percentage of verbs (predicative moods) is., on an average, under 15% of the total of words.

In the support of conjectures 1 and 2 we also mention:

- only one in six nouns is modified by an adjective, i.e. the role of the adjective diminishes and there are poems with no adjectives (see [3] - p.9, 12,20);

1.The "full" words category includes - according to the author - nouns, verbs (predicative moods only), adjectives and adverbs. The "empty" words category includes verbs (i.e.infinitives, gerunds, poet participles, supines), numerals, articles, pronuns, conjunctions, preopositions and interjections. The same terminology was also used by Solomon Marcus in his "Poetica matematica" published by Ed. Academiei, Bucharest, 197o (it wis translated in German and published by Athenäum, Frankfurt-am-Mein, 1973).

- on an average, there is one verb in a predicative mood in more then two lines, i.e.the role of the verbal predicate decreases und there are poems with no verbal predicates (se [3] - p.20);

From classicism to modernism both adjectives and verbal predicates graduaslly but constantly regressed).

- the poetry of the young; poets is characterized by economy of words and, implicitly, by the avoidance of the overused words; the adjectives were favoured by the romantics and the young poets feel the necessity to "renew" poetry.

-this renewal and effort to avoid the trivial may be also helpel by elimination of adjectives.

The strict use of adjectives or verbal predicates is also accounted for by the characteristics of the two main literary currents of our century.

a) hermetism - appeared after the World War I - consists, mainly in the hyper intellectualization of language and its codification; an adjective (i.e. an explanation concerningan object) or the predicative mood of a verb (strict definition of the gramatical tense) may diminish the degree of ambuguity, generalization or abstration intended by the poet.

b) surrealism - a literary of vanguard - saimed at detecting the irratonal, the uncenscious, the dream; because of its precise, definite character the adjective makes the reader "plunge" into the so carefully avoided real world.

CONJECTURE 3. In the recent Romanian poetry percentage of "full" words is over 55% of the total words.

Unlike in the spoken langurge in which the percentage of "full" and "empty" words is equal (see [1]) in poetry the percentage of "full" words is greater. This is lue to the fact that poetry is essence, it is dense, concentrated. The percentage of "full" words and the "density" of a literary work are directly proportional.

As a conclusion to the three conjectures we may say that:

- in its evolution from classicim to modernism the percentage of nouns increased, while that of a verbs decreased, less adverbs are used, on the other hand, because of the smaller number of verbs. In all, however, the percentage of "full" words increased.

3. The ferquency of the nouns with and without an article.

1. Percentage of nouns with an article	- 47.884%
2. Percentage of nouns without an article	- 52.116%

CONJECTURE 4. in the recent Romanian poetry the number of nouns with an article is, on an average, smaller than the number of those without an article. With an article the noun is more definite, specified which are characteristics undesirable from the same viewpoint as that mentioned above. That is why the indefinite article is favoured in modern poetry. The consequence of this preferred indefinite character of the noun enlarges the abstraction, generalization, ambiguity and, hence, the "density" of the poem. (see also the second part of assertions 1 and 2 and that the statistical conjecture 3). In its evolution from classicism to modernism the number of nouns without in article used in poetry also increased.

4. The frequency of nouns depending on the gramatical case they belong to.

Nominative	Genitive	Dative	Accusative	Vocative
29.497%	19.888%	0.335%	50.056%	0.224%
2	3	4	1	5

↑C L A S S I F I C A T I O N↑

CONJECTURE 5. In the poens under study, over 75% of the nouns are accusative or nomiative.

5. Sentences, lines, words. syllables, letters - average relationships

a)	2.402	letters/syllable
b)	1.933	syllables/word
c)	4.643	letters/word
d)	3.528	words/line
e)	6.820	syllables/line
f)	16.380	letters/line
g)	2.760	lines/sentence
h)	9.737	words/sentence
i)	18.823	syllables/sentence
j)	45.2o8	letters/sentence
k)	5.887	sentences/poem
l)	16.250	ines/poem
m)	57.330	wers/poem
n)	110.825	syllables/poem
o)	266.175	letters/poem

Conclusion: the poems are of medium length, the lines are short while the sentences are, again, of medium lenght.

6. The frequency of words according to their lenght (in syllables)

1 syllab,	2s.	3s.	4s.	5s.	6s.
41.509%	32.069%	19.363%	5.688%	1.371%	0.000%
order 1	2	3	4	5	6

The total number of syllables in the volume is ... 4,8oo. The frequency of worls and their length (in syllables) are in inverse ratio. Long words seem "less poetical".

CONJECTURE 6. In the recent Romanian poetry the percentage of words of one and two syllables is ... 75%. Again, it seens that short and very short words (of one and two syllables) seen more adequate to satisfy the internal rhythm of the poem. Longer words already have their own rhythm dictated by the juxteposition of the syllabels; it is very problable that this rhythm come into ... with the rhythm imposed by the poem. Shorter words are more easily uttered; longer words seem to render the text more difficult.

7. The frequency of words according to their length (in letters)

letter	1	2	3	4	5	6	7	8	9	10	11	12	13	14
	3.604%	25.426%	8.475%	11.089%	13.347%	13.149%	13.703%	5.861%	3.129%	1.149%	0.752%	0.237%	0.079%	0.000%
order	8	1	6	5	3	4	2	7	9	10	11	12	13	14

In the whole volume there are only two words of 13 leters and 6 of twelve. A... 90% of the words consist of no more thin 7 letters.

CONJECTURE 7. In the recent Romanian poetry the percentage of the two letter words is, on an average, about 25% of the words. On fact, the same percentage, oreven higher, is found in the ordinary language. Because of esthetic resors in poetry there is a slight tendency of reducing the frequency of the rwo lette words - which are, especially, prepositions and conjuntions -.

8.The frequency of the letters

The order of the letter	letter	the average % of the frequency of the letter	of the average % of vowels	The average % of cons
1.	E	11.994%		
2.	I	10.166%		
3.	A	8.406%		
4.	R	7.680%		
5.	N	6.407%		
7.	T	5.792%		
8.	L	5.237%		
9.	C	5.143%	46.865%	
1o.	S	4.220%		
11.	O	3.699%		
12.	P	3.451%		
13.	A	3.417%		53.135%
14.	M	3.178%		
15.	D	2.981%		
16.	T	2.828%		
17.	V	1.435%		
18.	G	1.4.8%		
19.	B	1.358%		
2o.	Ş	1.281%		
21.	F	1.179%		
22.	Z	0.846%		
23.	T	0.803%		
24.	H	0.496%		
25.	J	0.196%		
26.	X	0.034%		
27.	A	0.008%		
28– 31	K	0.000%		
28– 31	Q	0.000%		
28– 31	Y	0.000%		
28– 31	W	0.000%		

CONJECTURE 8. In the recent Romanian poetry the percentage of vowels is, on an average, over 45% of the total of letters.

Explanation: In the ordinary languarge the perrcentage of wowels is 42.7% (see [1]). In poetry it is greater because:

- vowels are more "musical" than consonants; therefore the words with more vowels "seem " more poetical; words with many vowels confer a special sonority to the text,

- modern poets and poetry are more preoccupied by form than by content, so that more attention is given to expression; the form may prejudice the content, because, very often, the reader is "caught" by sonority and less by essence.

- the internal rhythm of poetry, usually absent in the ordinary language is also conditioned, partially, by a greater number of vowels.

- rhyme, when used,also favours a grater percentage of vowels.

The percentage of vowels was greater in the period of classicim of poetry when the rhyth and rhyme were more frequently used. The special require ents of poetry impose a thorough filtration of the ordinary language.

Given the frequency of the letters in the Romanian language [1] in general:

1.E	5.N	9.L	13.D	17.S	21.F	25.J
2.I	6.T	10.S	14.P	18.B	22.T	16.X
3.A	7.U	11.O	15.M	19.V	23.Z	27.K
4.R	8.C	12.A	16.I	20.G	24.H	

we may calculate the deviation of this volume of verse from the ordinary language:

$$\alpha(v) = \frac{1}{27}\sum_{i=1}^{27}|\alpha(A_i)| \approx 0.741$$

where $\alpha(A_i)$ is the deviation of the letter A_i, $1 \le i \le 27$

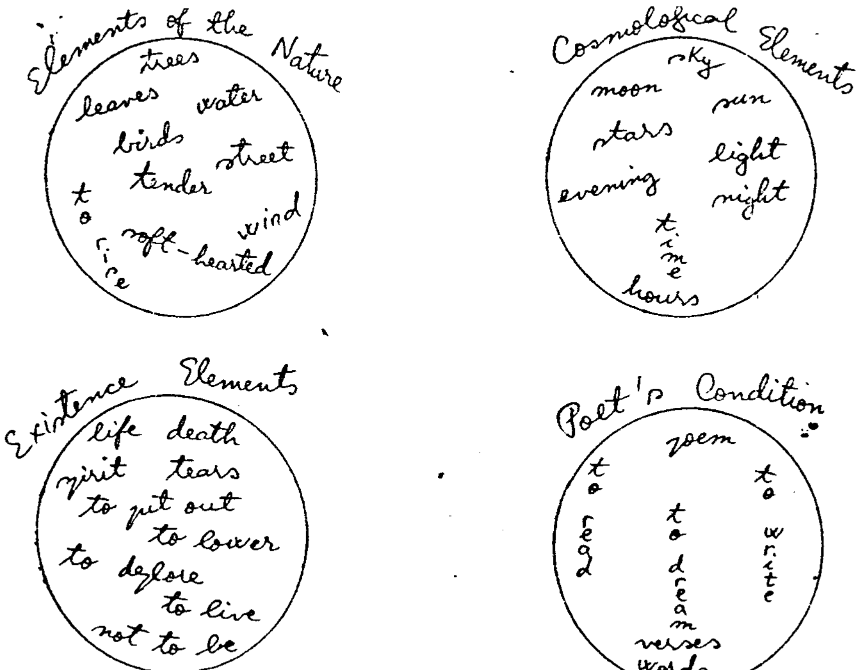
The informational energy, acording to O.Onicescu, is:

$\mathcal{E}(v) = \sum_{i=1}^{27} p_i^2 \approx$ 0.064 where p_i, $1 \le i \le 27$is the probability that the letter p_i may appear in the volume (see[1].

The first order entropy of the volume (according to Shannon) is:

$$H_1(v) = -\frac{1}{\log_{10} 2} \cdot \sum_{i=1}^{27} p_i \log_{10} p_i \approx 4.222$$

9. The themes of the volume are studied by determinig the recurrent elements, those that seem to obsess the poet. We will vall these elements "key-words" and they are, in order: nouns, verbs, adjectives. Their frequency in the volume is sudied. The more frequent words are all included in common notional spheres that will "decode" the themes dealt with by the poet in the volume under study, i.e.:



These 33 key-words (together with their synonyms) confer a certain pastoral note (this wa noticed by Constantin Matei, the newspaper "Înainte", Craiova), cosmological (Constantin M. Popa) existentialist nuances (Aureliu Goci, "Luceafărul", Bucharest); the preoccupation of the poet for the condition of the poet and society (Ion Pachia Tatomirescu, Craiova) is also revealed by the frequent use of certain suggestive words.

Of all the words, 33 key-words toghether with their synonyms nave the greatest frequency in the volume.

10.The frequency of worls and phrases strongly deviated from the "normal", i.e the rules of the literary language ia about 1.980 of the total of worls. (We mean expressions like: "state of self", "very near myself" , " it is raining at plus infinite" or words like "nontime", etc. (see [3], p. 9,29,40,31).

CONJECTURE 9. In the recent Romanian poetry the perecentage of words and phrases that strongy deviated from the "normal" of the ordinary language as well as the rules of the literary language is slightly over 1. This fact may be accounted for by:

- content seems less important; poets are more concerned with form;
- poets invent words and expressions to be able to better reveal their feelings and emotions;
- the asociation of antonyms may give birth to constructions that, seemhow "violate" the normal;
- poetry is, in fact, destined to break the rules and rebel aganist the ordinary fact (if, this right denied any newspaper article coull be called poetry).

"In art" said Voltaire, "rules are only meant to be broken".

In its evalution from clasicism to modernism the percentage of such abnormal words and construtions increased, starting, in fact, from zero. Kodern literary currents favour the appearance of then.

BIBLIOGRAPHY

[1] Marcus, Solomon - "Poetica matematică" - Ed. Academiei, Bucharest, 1970 (translated into german, Athenäum, Frankfurt-am-Mein, 1973).

[2] Marcus, Solomon - Edmond Nicolau - Sorin Stati - "Introducere în lingvistica matematică", Bucharest, 1966 (translated in Italian, Pătron, Bologna, 1971 and in Spanish, Teide, Barcelona, 1978).

[3] Florentin, Ovidiu - "Formule pentru spirit", Ed. Litera. Bucharest, 1981 (Translated in French, les Editions Express, Fès, Maroc, 1983); modern poems.

[4] Smarandache, Florentin - " A mathematical linguistic appoach to Rebus" - article published in"Revue roumaine de linguistique", tome XXVIII, 1983, collection"Cahiers de linguistique théorique et appliquée", tome XX, 1983, No,1 p,67-76.

[Editions Scientifiques, Casablanca, 1984]

A MATHEMATICAL LINGUISTIC APPROACH TO REBUS

INTRODUCTIION

The aim of paper is the investigation of some combinatorial aspects of written language, within the framework determined by the well-known game of crossword puzzles. Various types of probabilistic regularities appearing in such puzzles reveal some hidden, not well known restrictions operating in the field of natural languages. Most of the restrictions of this type are similar in each natural language. Our direct concern will be the Romanian language.

Our research may have some relevance for the phonostatistics of Romanian. The distribution of phonemes and letters is established for a corpus of a deviant morphological structure with respect to the standard language. Another aspect of our research may be related to the socalled tabular reading in poetry. The correlation horizontal-vertical considered in the first part of the paper offers some suggestions concerning a bidimensional investigation of the poetic sing.

Our investigation is concerned with the Romanian crossword puzzles published in [4]. Various concepts concerning crossword puzzles are borrowed from N.Andrei [3]. Mathematical lingustic concepts are borrowed from S,Marcus [1] and S.Marcus - E.Nicolau - S.Stati [2].

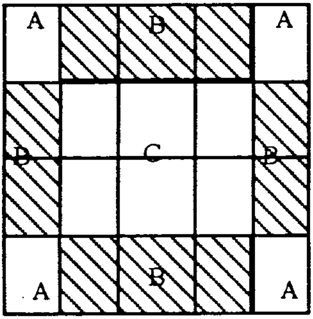
SECTION 1. THE GRILL

§ 1. MATHEMATICAL RESEARCHES ON GRILIS

It is known that a word in a grill is limited on the left and

right side either by a black point or by a grill final border.

We will take into account the words consisting of one letter (though they are not clued in the Rebus), and those of two (even they have no sense (e.g.N T, RU, ...)), three or more letters - even they represent that category of rare words (foreign localities, rivers etc., abbreviations etc. which are not found in the Romanian Language Dictionary (see [3], p.82-307 ("Rebus glossary")).



The grills have both across and down words.

We divide the grill into 3 zones:

a) the four peaks of the grill (zone A)

b) grill border (without the four peaks) (zone B)

c) grill middle zone (zone C)

We assume that the grill has n .. m (n lines and m columns) and p black points.

Then:

Proposition 1. The words overall number (across and down) of the grill is equal to $n + m + pNB + 2 \cdot pNC$,

where pNB = black points number in zone B,

pNC = black points number in zone C.

Proof: We consider initially the grill without any black point. Then it has $n + m$ words.

– If we put a black point in zone A, the words number is the same. (So it does not matter how many black points are found in zone A).

– If we put a black point in zone B, e.g. on line 1 and column j $i < j < m$, words number increases with one unit (because on line 1, two words werw formed (before there was only one), and on column j one word rests, too). The case is analog ous if we put a black point on column 1 and line $i, 1 < i < n$ (the grill may be reversed: the horizontal line becomes the vertical line and vice versa). Then, for each point in zone B a word is added to the grill words overall number.

– If we put a black point in zone C, let us say $i, 1 < i < n$, and column $j, 1 < j < m$, then the words number increses by two: both on line i and column j two words appear now, different from the previous case, when only one word was there on each line. Thus, for each black point in zone C, two words are added at the grill words overall number. From this proof results:

Corollary 1. Minimum number of words of grill $n \times m$ is $n + m$. Actually, this statement is achieved when we do not have any black point in zones B and C.

Corollary 2. Maximum number of words of a grill $n \times m$ having p black points is $n + m + 2p$ and it is achieved when all p black points are found in zone C.

Corollary 3. A grill $n \times m$ having p black points will have a minimum number of words when we fix first the black points in zone A, then in zone B (alternatively – because is not allowed to have two or more black points juxtaposed), and the rest in zone C.

Proposition 2. The difference between words number on the horizontal and on the vertical of a grill $n \times m$ is $n - m + pNBO - pNBV$,

where $pNBO$ = black points number in zone BO,

$pNBV$ = black points number in zone BV.

We divide zone B into two parts:

– zone $BO = B$ zone horizontal part (line 1 and n)

– zone $BV = B$ zone vertical part (line 1 and m).

The proof of this proposition follows the previous one and uses its results.

If we do not have any black point in the grill, the difference between the words on the horizontal and those on the vertical line is $n - m$.

- If we have a black point in zone A, the difference does not change. The same for zone C.

- If we have a black point in zone BO, then the difference will be $n - m - 1$. From this proposition 2 results.

Proposition 3. A grill $n \times m$ has $n + pNBO + pNC$ words on the horizontal and $m + pNBV + pNC$ words on the vertical.

The first solving method uses the results of propositions 1 and 2.

The second method straightly calculates from propositions 1 and 2 the across and down words number (their sum (proposition 1) and difference (proposition 2) are known).

Proposition 4. Words man length (=letters number) of a grill $n \times m$ with p black points is $\geq \dfrac{2(nm - p)}{n + m + 2p}$.

Actually, the maximum words number is $n + m + 2p$, the letters number is $nm - p$, and each letter is included in two words: one across and anther down. One grill is the more crossed the smaller the number of the words consisting of one or two letters and of black points (assuming that it meets the other known restrictions).

Because in the Romanian grills the black points percentage is max.

15% out of the total (rounding off the value at the closer

integer – e.g. 15% with a grill 13 × 13 equals 25.35 ≈ 25; with a grill 12 × 12 is 21.6 ≈ 22), so for the previous properties, for grills $n \times m$ with p black points we replace p by $\left[\frac{3}{20}\right]nm$, where $[x] = \max\{\alpha \in N \cdot |\alpha - x| \le 0.5\}$.

§2. STATISTIC RESEARCHES ON GRILLS

In [1] we find the notion "écart of a sound x", denoted by $\alpha(x)$, which equals the difference between the rank of x in Romanian and the rank of x in the analysed text.

We will extend this notion to the notion of *a text écart* which will be de noted by: $\alpha(t)$, and

$$\alpha(t) = \frac{1}{n}\sum_{i=1}^{n}|\alpha(A_i)|$$

where $\alpha(A_i)$ is A_i sound ecart (in [1]) and n represents distinct sounds number in text t. (If there are letters in the alphabet which are not found in the analysed text, these will be written in the frequency table giving them the biggest order.)

Proposition 1. We have a double inequalty: $0 \le \alpha(t) \le \frac{n-1}{2} + \frac{1}{n}\left[\frac{n}{2}\right]$ where $[y]$ represents the whole part of real nymber y.

Actually, the first inequalty is evident.

Let $\Phi = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$. Then $\sum_{i=1}^{n}|\alpha(A_i)| = \sum_{i=1}^{n}|i - j_i|$

This permutation constitues a mathematical pattern of the two frequency tables of sounds; in Romanian (the first line), in text t (the second line).

For permutation $\psi = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ n & n-1 & \dots & 2 & 1 \end{pmatrix}$ we have

$$\sum_{i=1}^{n} |i - j_i| = 2[(n-1)+(n-3)+(n-5)+\dots] = 2\sum_{k=1}^{\left[\frac{n}{2}\right]}(n-2k+1) =$$

$$=2\left[\frac{n}{2}\right]\left(n-\left[\frac{n}{2}\right]\right) = \frac{n(n-1)}{2} + \left[\frac{n}{2}\right],$$

where from $\alpha(t) = \frac{n-1}{2} + \frac{1}{n}\cdot\left[\frac{n}{2}\right]$.

By induction with respect to $n \geq 2$, we prove now the sum $S = \sum_{i=1}^{n} |i - j_i|$ has max. value for permutation ψ.

For $n = 2$ and 3 it is easily checked directly. Let us suppose the assertion true for values $< n + 2$. Let us show for $n + 2$:

$$\psi = \begin{pmatrix} 1 & 2 & \dots & n+1 & n+2 \\ n+2 & n+1 & \dots & 2 & 1 \end{pmatrix}$$

Removing the first and last column, we get:

$$\psi' = \begin{pmatrix} 2 & \dots & n+1 \\ n+1 & \dots & 2 \end{pmatrix},$$

which is a permutation of n elements and for which S will have the same value as for permutation

$$\psi'' = \begin{pmatrix} 1 & \dots & n \\ n & \dots & 1 \end{pmatrix},$$

i.e.max. value (ψ'' was obtained from ψ' by diminishing each element by one).

The permutation of 2 elements $\eta = \begin{pmatrix} 1 & n+2 \\ n+2 & 1 \end{pmatrix}$ gives maximum value for S. But ψ is achieved from ψ' and η:

The permutation of 2 elements $\eta = \begin{pmatrix} 1 & n+2 \\ n+2 & 1 \end{pmatrix}$ gives maximum value for S. But ψ is achieved from ψ' and η:

$$\psi(i) = \begin{cases} \psi'(i), & \text{if } \; i \notin \{1, n+2\} \\ \eta(i), & \text{contrary} \end{cases}$$

Remark: The bigger one text écart, the bigger the "angle of deviation" from the usual language.

It would be interesting to calculate, for example, the écart of a poem.

Then the notion of écart could be extended more:

a) *the écart of a word* being equal to the difference between word order in language and word order in the text;

b) *the écart of a text (ref. words)*:

$$\alpha_c(t) = \frac{1}{n} \sum_{i=1}^{n} |\alpha_c(a_i)|,$$

where $\alpha_c(a_i)$ is word a_i écart, and n – distict words number in text t.

*

We give below some rebus statistic data. By examining 150 grills [4] we pbtained the following results:

Occurrence frequency of words in the grill, depending on their lenght (in letters)

Letter order	Letter	Letter occurrence mean percentage	Vowels mean percentage	Consonants mean percentage
1	A	15.741%		
2	I	12.849%		
3	T	9.731%		
4	R	9.411%		

Letter order	Letter	Letter occurrence mean percentage	Vowels mean percentage	Consonants mean percentage
5	E	8.981%	47.462%	52.538%
6	O	5.537%		
7	N	5.053%		
8	U	4.354%		
9	S	4.352%		
10	C	4.249%		
11	L	4.248%		
12	M	4.010%		
13	P	3.689%		
14	D	1.723%		
15	B	1.344%		
16	G	1.290%		
17	F	0.860%		
18	V	0.806%		
19	Z	0.752%		
20	H	0.537%		
21	X	0.430%		
22	J	0.053%		
23	K	0.000%		

It is seen that a percentage of 49,035% consists of the words formed only of 1, 2 or 3 letters; – of course, there are lots of uncomplete words.

*

The study of 50 grills resulted in:

Occurrence fequency of letters in a grill (see next page)

It is noticed that vowels percentage in the grill (47.462%) exceeds the vowels percentage in language (42.7%).

So, we can generalize the following:

Statistical proposition (1): In a grill, the vowels number tends to be almost equal to 47.5% of the total number of the letters.

Here is some evidence: one word with n syllables has at least n vowels (in Romanian there is no syllable without vowel (see [2]).

The vowels percentage in Romanian is 42.7%; because a grill is assumed to from words across and down the vowels number will increase. Also, the last two lines and columns are endings of other words in the grill; thus they will have usually more vowels. When black points number decreases, vowels number will increase (in order to have an easier crossing, you need either more black points or more vewels). (A vowel has a bigger probability to enter in the componence of a word than a consonant.)

Especially in "record grills" (see [3], p. 33-48) the vowels and consonants alternace is noticed.Another criterion for estimating the grill value is the bigger deviation from this "statistical law " (the exception confirms the rule!): i.e. the smaller the vowel percentage in a grill, the bigger its value.

Statistical proposition (2): Generally the horizontal words number 73 equals the vertical one.

Here is the following evidence: 100 classical grills were experimenrally analysed, in [4], getting the percentage of 49.932% horizontal words. Usually the classical grills are square clues, the difference between the horizontal and vertical words being (see Proposition 2):

$$n - m + pNBO - pNBV = pNBO - pNBV .$$

The difference between the black points number in zone BO and zone BV can not be too big (± 1, ± 2 and rarely ± 3). (Usually, there are not many black points in zone B, because it iz not economical in crossing (see proof of Proposition 1)).

Taking from [1] the following letters frequency in language:

1. E	5. N	9. L	13. P	17. G	21. J
2. I	6. T	10. S	14. M	18. F	22. X
3. A	7. U	11. O	15. B	19. Z	23. K
4. R	8. C	12. D	16. V	20. H	

(because in the grill letters Ă, Â; Î; Ș; Ț; are replaced by A; I; S; T, respectively, in the above order they were cancelled) the ecart of the 150 grills becomes

$$\alpha(9) = \frac{1}{23}\sum_{i=1}^{23}|\alpha(A_i)| \approx 1{,}391;$$

the entropy is: $H_1 = -\frac{1}{109_{10}^{2}}\sum_{i=1}^{23} P_i \mathrm{Log}_{10} P_i \approx 3.865$

and the infomational energy (after O. Onicescu) is: $E(g) = \sum_{i=1}^{23} P_i^2 \approx 0.084.$

Examining 50 grills we got:

Words frequency in a grill with respect to the syllables number

Mean percentage of occurrence of a word in a grill								Mean length of a word in sylla-bles
1 syllable	2	3	4	5	6	7	8	
35.588%	26.920%	21.765%	9.551%	5.294%	0.882%	0.000%	0.000%	2.246

(in the category of the one syllable-words, the words of one, two or. three letters, without any sense – rare words – were also considered.) It is seen that the percentage of words consisting of one and two syllables is 62.508% (high enough).

Another statistics (of 50 grills), concerning the predominant parts of speech in a grill has estabished the first three places:

1. nouns 45.441%
2. verbs 6.029%
3. adjectives 2.352%

Notice the large number of nouns.

*

SECTION II. REBUS CLUES

§ 1. STATISTICAL RESEARCHES ON REBUS CLUES

Studying the clues of 100 "clues grills", the following statistical data resulted:

Rebus clues frequency according to their length (words number)

It is noticed that the predominant clues are formed of 2, 3, or 4 words. For results obtained by investigating 100 "clues grills", see next page.

It is worth mentioning that vowels percentage (46.467%) from rebus clues exceeds vowels percentage in the language (42.7%).

By calculating the clues écart (in accordance with the previous formula) it results:

$$\alpha(dr) = \frac{1}{27}\sum_{i=1}^{27}|\alpha(A_i)| \approx 1.185$$

(sound frequency used by Solomon Marcus in [1] was used here), the entropy (Shannon) is:

$$H_1 = -\frac{1}{\mathrm{Log}_{10}^2}\sum_{i=1}^{27}p_i \log_{10} p_i \approx 4.226$$

and informational energy (O.Onicescu) is:

$$E(dr) = \sum_{i=1}^{23}p_i^2 \approx 0.062.$$

(The calculations were done by means of a pocket calculator).

Letters occurrence frequency in the rebus clues

Letter order	Letter	Mean percentage of letter occurrence in clues	Vowels percentage	Consonants mean percentage	Letters no. (mean) necessary to clue a grill	Mean length of a word (in letters) used in clues
1	E	10.996%				
2	I	9.778%				
3	A	9.266%	46.679%	53.321%	657.342	4.374
4	R	7.818%				
5	U	6.267%				
6	N	6.067%				
7	T	5.611%				
8	C	5.374%				
9	L	4.920%				
10	O	4.579%				
11	P	4.027%				
12	Ă	3.992%				
13	S	3.831%				
14	Î	3.309%				
15	D	3.079%				
16	Î	1.801%				
17	V	1.527%				
18	F	1.449%				
19	Ş	1.360%				
20	Ţ	1.338%				
21	G	1.330%				
22	B	1.238%				
23	H	0.532%				
24	J	0.358%				
25	Z	0.092%				
26	X	0.037%				
27	K	0.024%				

REFERENCES

1. Marcus, Solomon - Poetica matematică, Ed. Academiei, Bucureşti, 1970 (German translation, Athenäum, Frankfurt am Main, 1973).

2. Marcus, Solomon, Edmond Nicolau, S,Stati - Introducere în lingvistica matematică, Bucureşti, 1966 (Italian translation, Patron, Bologna, 1971; Spanish translation, Teide, Barcelona, 1978).
3. Andrei, Dr. N. - Îndreptar rebusist, Ed. Sport-Turism, Bucureşti, 1981.
4. "Rebus" magazine collection, Bucureşti, 1979-1982.
The Craiova University
Natural Sciences Department

[Published in "Revue Roumaine de linguistique", Tome XXVIII, 1983, "Cahiers de linguistique theorique et appliquee", Bucharest, Tome XX, 1983, No. 1, pp. 67-76.]

HYPOTHESES SUR LA DETERMINATION D'UNE REGLE POUR LES JEUX DE MOTS CROISES

Les problèmes de mots croisés sont composés, on le sait, de griles et de définitions. Dans la langue roumaine on impose la condition que le pourcentage de cases noires par rapport au nombre total de cases de la grille ne depasse pas 15%.

Pourquoi 15%, et pas plus ou moins? C'est la question a laquelle cet article tente de repondre. (Cette question est dûe au Professeur Solomon NARCUS - symposium national de Mathematiques "Traian Lalesco", Universite de Craiova, 10 juin 82.)

Voici tout d'abord un tableau qui présente de manière synthetique une statistique sur le grilles contenant un tres faible pourcentage de cases noires (of. [2], pages 27-29):

LES GRILLES -RECORDS:

Dimension de la grille	Nombre minimum de cases noires enregistré	Pourcentage de cases noires	Nombre des grilles–records réalisées au 1 iuin 82
8x8	0	0,000%	24
9x9	0	0,000%	3
10x10	3	3,000%	2
11x11	4	3,305%	1
12x12	8	5,555%	1
13x13	12	7,100%	1
14x14	14	7,142%	1
15x15	17	7,555%	1
16x16	20	7,812%	2

Dans ce tableau, plus la dimension est grande, plus de pourcentage de cases noires augmente, parce que le nombre de mots de grande longueur est reduit.

Les dimensions courantes des grilles vont de 10x10 a 15x15.

On peut remarquer que le nombre des grilles ayant un pourcentage de cases noires inferieur a 8% est tres reduit: les totaux de la derniere colonne cumulent toutes les grilles realisées en Roumanie depuis 1925 (apparition des premiers problemes de mots croises en Romanie), jusqu'a nos jours. On voit donc que le nombre des grilles-records est négligeable quand on le compare aux milliers de grilles créees. Pour cette raison, la regle qui imposait le pourcentage des cases noires, devait l'établir superieur a 8%. Mais les mots croises etant des jeux, devaient gagner un large public, il ne fallait donc pas rendre les problemes trop dificiles.

D'ou un pourcentage de cases noires au moins egal a 10%.

Ils ne devainet pas non plus etre trop faciles, c'est-a-dire ne nécessiter aucun effort de la part de celui qui les composerait, d'ou un pourcentage de cases noires inferieur a 20%. (Sinon en effet il devient possible de composer des grilles formées en totalité de cases mots de 2 ou 3 lettres).

Pour soutenir la deuxième assertion, on a établi que la longueur moyennne des mots d'une grille nxm avec p cases noires est sensiblement egale a $\frac{2(n\cdot m-p)}{n+m+2p}$ (of. [3], § 1, Prop,4). Pour nous, p est 20% de n.m, il en résulte que

$$\frac{2(n\cdot m-\frac{20}{100}n\cdot m)}{n+m+2\frac{20}{100}n\cdot m}\leq 3\Leftrightarrow\frac{1}{n}+\frac{1}{m}\geq\frac{2}{15}.$$

Donc pour des grillesc courantes ayant 20% de cases noires, la longueur moyenne des mots serait inferieure a 3.

Meme dans les commencements des jeux de mots croises, le pourcentage de cases noires n'etait par trop grand: ainsi dans une grille de 1925 de 11x11, on compte 33 cases noires, soit un pourcentage de 27,272% (of. [2], p.27).

En se developpant, ce jou s'est impose des conditions "plus fortes" - c'est-a-dire une diminution des cases noires.

Pour choisir un pourcentage entre 10 et 20%, il ne reste plus qu'a supposer que la predilection des gens pour les chiffres ronds a joué (les mots croises sont un jeu, pas besoin de la précision mathematique de sciences). D'ou la regle des 15%.

Une statistique (of. [3], § 2), montre que le pourcentage de cases noires dans les grilles actualles est de environ 13,591%. La règle est donc relativement aisée a suivre et ne peut qu'attirer de nouveaux cruciverbistes.

Pour repondre completement a la question posée, il faudrait considérer aussi certains aspects philosophiques, psychologiques, et surtout sociologiques, surtout ceux liés a l'histoire de ce jeu, a son developpement ulterieur, aux traditions.

Bibliographie:

[1] Marcus Solomon, Edmond Nicolau, S.Stati - "Introducere în lingvistica matematică", Bucarest, 1966 (traduit en italien, Patron, Bologna, 1971: en espagnol, Teide, Barcelona, 1978).

[2]Andrei, Dr.N. - "Îndreptar rebusist", Editura Sport-Turism, Bucarest, 1981.

[3] Smarandache, Florentin – "A mathematical linguistic approach to Rebus", publié dans la "Revue roumaine de linguistique", Tome XXVIII, 1983, collection "Cahiers de linguistique theorique et appliquee", Tome XX, 1983, no.1, p. 67-76, Bucarest.

[Publié dans le " Caruselul enigmistic", Bacău, Nr. 5, 1086, 2-6 mai, pp. 29 et 31.]

LIMBAJUL DEFINIȚIILOR REBUSISTE SPIRITUALE

„Limbajul rebusist“ este undeva la granița dintre limbajul ștințific și cel poate, având multe lucruri comune și cu limbajul uzual și chiar muzical.(jocurile, deoarece au o anumită rezonanță acustică).

În timp ce carențele semantice având definiții directe (aproape de dicționar [3], p.50-56) al unui limbaj apropiat de cel științific (chiar și de cel uzual prin modul simplu de exprimare) la "careurile de definiții". Limbajul este apropiat de cel poetic. Există chiar definiții literare. (vezi [3] p.57, [4] care utilizează procedeele stilistice literare: ca metafora, comparația, alegoria, practică etc. Mai departe vom face o PARALELĂ ÎNTRE LIMBAJUL ȘTIINȚIFIC, LIMBAJUL POETIC, LIMBAJUL REBUSIST ("CAREURILE DE DEFINIȚII") urmărind îndeaproape regulile din [1] (cap. "Opoziții între limbajul științific și cel poetic"), rezultate pe care le vom restrânge și asupra limbajului rebusist.

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-ipoteză rațională	-ipoteză emoțională	-ipoteză rațională + emoțională (citind definiția, te gândești o clipă, uneori o iei pe-o pistă greșită; când greșești răspunsul (cuvântul corespunzător din grilă, te luminezi, entuziasmezi)

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-densitate logică	-densitate de sugestie	-densitate logică + sugestia (definiția trebuie ca în termeni cât mai puține să spună cât mai mult – densitate logică); să fie cât mai inedită, mai luminoasă, emoținantă (densitate de sugestie)
-sinonimie infinită	-sinonimie absentă	-sinonimie redusă (nici chiar infinită, dar nici absurdă); (nu același cuvânt din grilă poate avea mai multe definiții rebusiste; însă o definiție se exprimă aproa-pe unic, deci sinonimia este aproape absentă)
-anonimie absentă	-anonimie infinită	-anonimie mare (nici absentă dar nici infinit) (în cazul def. semnificația depinde de autor: chiar dacă cititorul înțelege altceva va inter-veni partea rațională, cuvântul să se potri-vească în grilă la locul cuvenit, chiar definițiile literale, în careuri nu mai au o anonimie infinită pentru că aici intervine și partea rațională:

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
		găsirea neapărat a unui răspuns; în cazul care-urior tematice definiții directe, anonimia este aproape absentă).
-artificial	-natural	-natural și artificial (în general definițiile au caracter natural; dar definițiile bazate pe jocuri de litere (ex. definiția "Începe noaptea" are răspunsul "NO" au un caracter artificial).
-general	-singular	-singular și general (doar definițiile bazate pe jocul de litere pot avea un caracter general).
-traductibil	-netraductibil	-traductibil (în sensul că definiția are o semnificație logică).
-prezența problemelor de stil	-absența problemelor de stil	-absența problemelor de stil (aceeași definiție nu poate fi spusă fără a-i schimba nuanța – pe când un cuvânt din grilă poate fi definit în mai multe feluri).

LIMBAJUL ŞTIINŢIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-finitate în spaţiu, constantă în timp	-variabilitate în spaţiu şi timp	-variabilitatea în spaţiu şi în timp, variabilitate mai mică decât cea de la limbajul poetic.
-numărabil	-nenumărabil	-nenumărabil
-transparent	-opac	-semiopac (sau semitransparent la început def. pare opacă, până se găseşte răspunsul).
-tranzitiv	-reflexiv	-reflexiv (fac excepţie din nou definiţiile bazate pe jocuri de litere, care au şi un caracter tranzitoriu)
-independenţa de expresie	-dependenţa de expresie	-dependenţa de expresie.
-independenţă de structura muzicală	-dependenţă de structură muzicală	-dependenţă de structură muzicală.
-paradigmatic	-sintagmatic	-sintagmatic

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-concordanță între distanța paradigmatică și sintagmatică	-neconcordanță între dinstanța paradigmatică și sintagmatică	-distanța paradigmatică și sintagmatică (sunt împerecheri de cuvinte diferite, jocuri de cuvinte, procedee folosite ca în poezie)
-contexte scurte	-contexte lungi	-contexte scurte (1) (aici se apropie de limbajul științific, pentru că se are în vedere proverbul: ”Non multa sed multum”; din investigațiile statistice anterioare a rezultat că lungimea medie a unei definiții rebusiste (spirituale) este 4,192 cuvinte: definițiile cu jocurile de litere au de obicei foarte puține cuvinte.

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-dependență contextuală	-tinde spre independență pendența de expresie	-independență contextuală (în cazul careurilor tematice ce este și o mică dependență; de asemenea, există și cazuri mai rare când o definiție depinde de cea anterioară (definițiile cu jocuri de litere sau cuvinte – de obicei)).
-logic	-alogic	-logic
-denotație	-anotație	-conotație (dacă o definiție ar da sensul direct al unui cuvânt am avea definiții directe (ca la dicționar) și atunci și-ar pierde total ”surpriza”., ”spiritualitatea”, ”ingeniozitatea”, ”spontaneitatea” la careurile tematice definițiile cu caracter denotativ.

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-rutină	-creație	-creație și... experiență (că să nu zicem rutină!)
-stereotipii generale	-stereotipii personale	-stereotipii personale (există chiar așa numitele careuri "în manieră personală" – vezi [3]. p.56-58)
-explicabil	-inefabil	-inefabil... care o explică! (definiția luată separat, ne-privită ca o "între-bare" este inefabilă luată împreună cu răspunsul devine explicabilă: în general, definiția prezintă și un grad de ambiguitate (mai multe piste pe care te poate îndruma) – altfel ar fi banală – un grad de nedeterminare: se folosește de multe ori sensul propriu în locul celui figurat sau reciproc definită are însă și o logică a ei, logică ce devine palpabilă odată cu aflarea răspunsului).

LIMBAJUL ȘTIINȚIFIC	LIMBAJUL POETIC	LIMBAJUL REBUSIST
-luciditate	-vrajă	-vrajă – luciditate (conform celor imediat anterioare) (la început limbajul rebusist, domină pe om, până află "cheia" când omul va ajunge să domine la rândul lui – limbajul poetic
-previzibil	-imprevizibil	-imprevizibil la început, previzibil după dezlegare: (imprevizibil convenit în previzibil)
-explicabi	-inefabil	

CONSIDERAȚII ASUPRA LIMBAJULUI ȘTIINȚIFIC ȘI "LIMBAJULUI LITERAR"

Cum nimic în natură nu este absolut, evident nu va exista o graniță precisă între limbajul științific și cel "literar" (limbajul folosit în literatură): Deci vor fi zone în care cele două zone se intersectează.

În [1], capitolul "Apariții între limbajul științific și cel poetic", Solomon Marcus prezintă deosebirile între cele două, deosebiri care fac totuși și o apreciere între ele.

În continuare vom glasa puțin pe marginea acestui material, prezentând părți comune ale limbajului științific și cel literar:

- amândouă caută noul, ineditul

- amândouă presupun o creație (rezolvarea unei probleme înseamnă creație: scrierea unei propoziții de asemenea)

- atât literatura cât și știința au o artă de a fi predate, învățate, tudiate (metodica predării aritmeticii, a limbii române etc.)

- și în știință există o estetică (de ex. "estetica matematică") i în literatură există o logică (chiar și absurdul lui Eugen onescu, miturile lui Mircea Eliade au o logică a lor, aparte: nalog putem extinde ideea la dadaismul lui Tristan Tzaia are o numită logică (de construcție; se decupează cuvinte din ziare și e amestecă formând apoi versuri)

- dezvoltarea științei implică dezvoltarea literaturii într-un nume sens: a apărut astfel, literatura științifico-fantastică în crierile literare ce folosesc informații obținute de către știință: teratură (contemporană) tratează și probleme din știință (ex. ugustin Buzura a scris romanul "Absenții" descriind viața nui cercetător în medicină: poetul inginer George Stanca ntroduce termeni tehnici în poeme cu vers din volumul său "Tandrețe maximă" sună așa: $\sin^2 x + \cos^2 x = 1$"!) analog poetul inginer Gabriel Chifu (volumul "O interpretare a purgatoriului") și profesorul de matematică Ovidiu Florentin, autor al volumului chiar intitulat "Formule pentru spirit" – fiecare poem fiind considerat ca "o formulă" de moment (depinzând de timp, loc, spațiu, individ) pentru spirit;

- însăși scrierea unor romane contemporane inspirate din viața muncitorilor, țăranilor necesită o documentare științifică din partea literaților.

Literatură influențează la știință o anumită estetică: există și metafore matematice (vezi [1], [2]) și în general am zice "metafore științifice", nu se știe ce idei descoperirea unor relații în știință Gradul de înțelegere (exegeză) a unei poezii și a unui text literar în general, depinde și de gradul de cultură al fiecăruia de inițierea lui (stadiul în domeniul respectiv), de cunoștințele sale științifice.

- există mulți oameni de știință care pe lângă articolele lor științifice scriu și literatură sau domenii înrudite (ex. cartea de memorii a academicianului (matematician) Octav-Onicescu "Pe drumurile vieții", renumitul medic român Gheorghe Marinescu scrie poeme (folosind cuvinte dacice) sub pseudonimul George Dinizvor, marele Ion Barbu - Dan Barbilian a excelat și-n poezie și în matematică. Marele poet Vasile Voiculescu a fost și un bun medic; iar profesorul de matematică Aurel M. Buricea scrie versuri, analog matematicianul Ovidiu Florentin–Florentin Smarandache scrie poeme și articole de matematică; în literatura străină găsim poetul–matematician Omar Khajyom și Lewis Carroll - Charles L. Dodgson) însă literați care să facă și cercetări în științele fundamentale sau tehnice nu prea există!

BIBLIOGRAFIE:

[1] Marcus, Solomon - "Poetica matematică", Ed. Academiei, București, 1970.
[2] Marcus, Solomon - "Introducere în lingvistica matematică", București, 1966.
[3] Andrei, Dr.N. - "Îndreptar rebusist", Ed. Sport-Turism, București, 1981.
[4] colecția revistei "Rebus", 1979-1982.
[5] Marcus, Solomon - "Limbajul poetic-limbajul matematic", în revista "Orizont" (Timișoara) din 26 martie 1982.

LA FREQUENCE DES LETTRES (PAR GROUPES EGAUX) DANS LES TEXTES JURIDIQUES ROUMAINS

Analysant le degré de détérioration des touches d'une machine à écrire qui a fonctionné plus de 40 ans au greffe d'un tribuunal d'un district roumain (Vilcea), on les a réparties dans les groupes suivants:

1) Lettres completement deteriorees (on ne peut plus rien lire sur la touche).
2) Lettres dont on voit un seul point, a peine perceptible.

....

10) Lettres dont il manque un seul point.
11) Lettres qui se voient parfaitement, sens aucun manque.
12) Lettres qui, n'étant presque pas utilisées, étaient convertes de poussiere.

On a obtenu les resultats suivants:

1) E, A	7) O,C,U,D,Z,
2) I	8) N
3) R	9) L
4) T	10) V,M
5) S	11) F,G,B,H,X,J,K
6) P	12) W,Q,Y

Cette classification est un peu differente de celle de [1], parce que les lettres A, Ă, Â sont ici cumulées en une seule lettre: A, de meme I et I dans I, S et Ş dans S, T et Ţ dans T.

En étudiant l'écart de ces texte (of. [2]), on obtient:

$$\alpha(j) = \frac{1}{23}\sum_{i=1}^{23}|\alpha(A_i)| \approx 2,348,$$

donc l'écart du langage juridique des fréquences courantes de la langue est beaucoup plus grand que celui du langage des mots croisés: $\alpha(g) \approx 1,391$ et $\alpha(d_r) \approx 1,185$.

Les sauts les plus spectaculaires sont réalisés par les lettres P, Z et N:

$\alpha(P) = 6$, $\alpha(Z) = 7$, $\alpha(N) = -8$.

Cet article surprend peut-etre par sa banalité. Mais, alors que les autres auteurs ont fait des mois de calculs a l'aide d'ordinateurs,choisissant certains livres et faisant compter les lettres (!) par l'ordinateur,moi j'ai déduit cette fréquence des lettres en quelques minutes (!), par une simple obsevation.

Bibliographie:

[1] Marcus, Solomon - "Poetica matematică", Editura Academiei, Bucarest, 1970 (traduit en allemand, Athenäum, Frankfurt, 1973).

[2] Smarandache, Florentin - " A mathematical linguistic approach to Rebus", Tome XXVIII, 1983, la collection "Cahiers de linguistique théorique et appliquée", Tome XX, 1983, No.1, p. 67-76, Bucarest.

MATHEMATICAL FANCIES AND PARADOXES

?resented at "The Eugene Strens Memorial on Intuitive and ?ecreational Mathematics and its History," University of ?algary, Alberta, Canada; July 27-August 2, 1986.
?artly "published in "Beta", Craiova, 1987; "Gamma", Brașov, 987; and "Abracadabra", Salinas (California), 1993-4.]

MISCELLANEA

1. Archimedes' "fixed point theorem": "Give me a fixed point in space, and I shall upset the Earth,"

2. MATHEMATICAL LINGUISTICS[1]

Poem by Ovidiu Florentin[2]

Definition

A word's sequence converges if it is found in a neighborhood of our heart..

*

The hermetic verses are linear equations.

*

Theorem

For any X there is no y such that Y knows everything which X knows. And the reciprocal.

The proof is very intricate and long, and we will present it. We leave it to the readers to solve it!

**

Smarandache's law: Give me a point in space and I shall write the proposition behind it.

Final Motto

- -O, MATHEMATICS, YOU, EXPRESSION OF THE ESSENTIAL IN NATURE!

---

1 Volume which includes this mathematical poem (pp. 39-41).

2 (Translated from Romanian by the author.) It is the matematician's literary pseudonym. He wrote many poetical volumes (in Romanian and French), as "Legi de composiţie internă. Poeme cu . . . probleme!" (Laws of internal composition. Poems with . . . problems!), Ed. El Kitab, Fès, Morocco, 1982.

AMUSING PROBLEMS

1. Calculate the volume of a square.

(Solution: Volume=Area of the Base x Height = Side^2 x 0=0! We look at the square as an extreme case of parallelepiped with the height null.)

2. ?x7=2?

(Solution: Of course $\frac{2}{7}$ x7=2!)

3. Ten birds are on a fence. A hunter shoots three of these. How many birds remain?

(Answer: **None**, because the three dead birds fell down from the fence and the other seven flew away!)

4. Ten birds are in a meadow. A hunter shoots three of these. How many birds remain?

(Answer: three birds, the dead birds, because the others flew away!)

5. Ten birds are in a cage. A hunter shoots three of these. How many birds remain?

(Answer: **ten birds**, dead and living, because none can get out!)

6. Ten birds are in the sky. A hunter shoots three of these. How many birds remain?

(Answer: **seven birds**, at last, those who are still flying and those that fell down!)

7. Prove that the equation $X = X + 2$ has two distinct solutions.

(Answer: $X = \pm\infty$!)

8. (Solving Fermat's last theorem:) Prove that for any non-null integer n, the equation $X^n + Y^n = Z^n$, $XYZ \neq$, has at least one integer solution!

(Answer: (a) $n \geq 1$. Let $X_k = Y_k = Z_k = 2^k$, $K = 1, 2, 3, \ldots$ All $X_k \in N$, $K \geq 1$. $L = \lim_{K \to \infty} X_k \in N$. But $L = \infty \in N$, that is the integer infinite, and $\infty^n + \infty^n = \infty^n$! If n is even, the equation has eight distinct integer solutions: $X = Y = Z = \pm\infty$! Similarly we take the negative integer infinite: $-\infty \in \mathbf{Z}$ $-\cdot]$ (b) $n \leq -1$. Clearly there are at least eight distinct integer solutions: $X = Y = Z = \pm\infty$!)

OU SE TROUVE LA FAUTE? (EQUTIONS DIOPHANTIENNES)

Enoncé:

(1) Résoudre dans $\mathbf{Z}$ l'équation: $14x + 26y = -20$.

"Résolution": La solution générale entière est:

$$\begin{cases} x = -26k + 6 \\ y = \ \ 14k - 4 \end{cases} \quad (k \in \mathbf{Z})$$

(2) Résoudre dans $\mathbf{Z}$ l'équation: $15x - 37y + 12z = 0$.

"Résolution" La solution générale entière est:

$$\begin{cases} x = k + 4 \\ y = 15k \qquad (k \in \mathbf{Z}) \\ z = 45k - 5 \end{cases}$$

(3) Résoudre dans $\mathbf{Z}$ l'équation: $3x - 6y + 5z - 10w = 0$.

"Résolution"l'équation s'écrit:

$3(x - 2y) + 5z - 10w = 0$.

Puisque x,y,z,w sont des variables entières, il en résulte que 3 divise z et que 3 divise w. C'est-à-dire:

$z = 3t_1 (t_1 \in \mathbf{Z})$ et $w = 3t_2 (t_2 \in \mathbf{Z})$

Donc: $3(x - 2y) + 3(5t_1 - 10t_2) = 0$ ou $x - 2y + 5t_1 - 10t_2 = $ $=0$.

Alors: $\begin{cases} x = 2k_1 + 5k_2 - 10k_3 \\ y = k_1 \\ z = 3k_2 \\ w = 3k_3 \end{cases}$ avec $(k_1,k_2,k_3) \in Z^3$ constitue la solution générale entière de l'equation.

Trouver la faute de chaque "résolution"?

SOLUTIONS.

(1) $x = -26k + 6$ et $y = 14k - 4$ ($k \in \mathbf{Z}$). est une solution entière pour l'équation (parce qu'elle la vérifie), mais elle n'est pas la solution générale: puisque x=-7 et y=3 vérifient l'équation, ils en sont une solution entière particulière, mais:

$\begin{cases} -26k + 6 = -7 \\ 14k - 4 = 3 \end{cases}$ implique que k=1/2 (n'appartient pas a $\mathbf{Z}$).

Donc on ne peut pas obtenir cette solution particulière de la "solution générale" antérieure.

La vraie solution générale est: $\begin{cases} x = -13k + 6 \\ y = 7k - 4 \end{cases}$ ($k \in \mathbf{Z}$). (of [1])

(2) De meme, x=5 et y=3 et z=3 est une solution particulière de l'equation, mais qui ne peut pas se tirer de la "solution générale" puisque: $\begin{cases} k + 4 = 5 \Rightarrow k = -1 \\ 15k = 3 \Rightarrow k = 1/5 \\ 45k - 5 = 3 \Rightarrow k = 8/45 \end{cases}$, contradictions.

La solution generale entiere est: $\begin{cases} x = k_1 \\ y = 3k_1 + 12k_2 \\ z = 8k_1 + 37k_2 \end{cases}$

(avec $(k_1,k_2) \in \mathbf{Z}^2$, cf. [1].

(3) L'erreur est que: "3 divise (5z-10w)" n'implique pas que

"3 divise z et 3 divise w". Si on le croit on perd des solutions, ainsi (x,y,z,w)= (-5,o,5,1) constitue une solution entière particulière qui ne pas s'obtenir a partir de la "solution" de l'énoncé.

La résolution correcte est:

$3(x-2y)+5(z-2w)=0$, c'est-a-dire $3p_1+5p_2=0$,avec $.p_1=x-2y$ dans $\mathbf{Z}$, et $p_2=z-2w$ dans $\mathbf{Z}$.

Il en résulte: $\begin{cases} p_1 = -5k = x-2y \\ p_2 = 3k = z-2w \end{cases}$ avec $\mathbf{Z}$.

D'ou l'on tire la solution generale entière:

$$\begin{cases} x = 2k_1 - 5k_2 \\ y = k_1 \\ z = \quad 3k_2 + 2k_3 \\ w = \quad k_3 \end{cases} \text{avec } (k_1,k_2,k_3)\in\mathbf{Z}^3$$

[1] On peut trouver ces solutions en utilisant:
Florentin SMARANDACHE - "Un algorithme de résolution dans l'ensemble des nombers entiers pour les équations linéaires".

OU SE TROUVE LA FAUTE SUR LES INTEGRALES ???

Soit la fonction $f:\mathbf{R}\to\mathbf{R}$, définie par $f(x)=2\sin x\ \cos x$.

Calculons la primitive de celle-ci:

(1) Première méthode.

$\int 2\sin x\ \cos x\ dx = 2\int u\ du = 2\frac{u^2}{2} = u^2 = \sin^2 x$, avec $u=\sin x$.

On a donc $F_1(x) = \sin^2 x$.

(2) Deuxième méthode:

$\int 2\sin x \ \cos x \ dx = -2\int \cos x(-\sin x)dx = -2\int v \ dv = -v^2$,

donc $F_2(x) = -\cos^2 x$.

(3) Troisième méthode:

$\int 2\sin x \ \cos x \ dx = \int \sin 2x \ dx = 1/2\int(\sin 2x) \ 2dx =$

$= 1/2\int \sin t \ dt = -1/2\cos t$ donc $F_3(x) = -1/2\cos 2x$.

On a ainsi obtenu 3 primitives differentes de la même fonction.

Comment est-ce possible?

Réponse: Il n'y a aucune faute! On sait qu'une fonction admet une infinité de primitives (si elle on admet une), qui ne diffèrent que par une constante.

Dans notre exemple on a:

$F_2(x) = F_1(x) - 1$ pour tout réel x,

et $F_3(x) = F_1(x) - 1/2$ pour tout réel x.

OU SE TROUVE LA FAUTE DANS CE RAISONNEMENT PAR RÉCURRENCE ???

A un concours d'entrée en faculté on a pose le problème suivant:

"Trouver les polynômes $P(x)$ a coefficients réels tels que $xP(x-1) = (x-3)P(x)$, pour tout x réel."

Quelques candidats ont cru pouvoir démontrer par récurrence que les polynômes de l'énoncé sont ceux qui vérifient la propriété suivante: $P(x) = 0$ pour tout contier naturel.

En effet, disent ils, si on pose $x = 0$ dans cette relation, il en résulte que $0 \cdot P(-1) = -3 \cdot P(0)$, donc $P(0)=0$.

De même, avec $x = 1$, on a:

$1 \cdot P(0) = -2 \cdot P(1)$, donc $P(1) = 0$, etc. . .

On suppose que la propriété est vraie pour $(n-1)$, càd que $P(n-1) = 0$, et on regarde ce qu'il on est pour n:

On a: $n \cdot P(n-1) = (n-3) \cdot P(n)$, et puisque $P(n-1) = 0$, il en résulte que $P(n) = 0$.

Où la démonstration peche-t-elle ???

Reponse: Si les candidats avaient essayé le rang $n = 3$, ils auraient trouvé:

$3 \cdot P(2) = 0 \cdot P(3)$ donc $0 = 0 \cdot P(3)$, ce qui n'entraîne pas que $P(3)$ est nul: en effet cette egalité est vraie pour tout réel $P(3)$.

L'erreur provient donc de ce que l'implication:

"$(n-3) \cdot P(n) = n \cdot P(n-1) = 0 \Rightarrow P(n) = 0$" n'est pas juste.

On peut trouver facilement que $P(x) = x(x-1)(x-2)k$, $k \in \mathbf{R}$

UNDE ESTE GREȘEALA?

Se consideră funcțiile $f, g: \mathbf{R} \to \mathbf{R}$, definite astfel:

$$f(x) = \begin{cases} e^x, & x \le 3 \\ e^{-x}, & x > 3 \end{cases} \quad \text{și} \quad g(x) = \begin{cases} x^2, & x \le 0 \\ -2x+7, & x > 0 \end{cases}$$

Să se calculeze fog.

"Soluție." Putem scrie:

$$f(x) = \begin{cases} e^x, & x \le 0 \\ e^x, & 0 < x \le 3 \\ e^{-x}, & x > 3 \end{cases} \quad \text{și} \quad g(x) = \begin{cases} x^2, & x \le 0 \\ -2x+7, & 0 < x \le 3 \\ -2x+7, & x > 3 \end{cases}$$

De unde

$$fog(x) = f(g(x)) = \begin{cases} e^{x^2}, & x \le 0 \\ e^{-2x+7}, & 0 < x \le 3 \\ e^{2x-7}, & x > 3 \end{cases}$$

și $fog: \mathbf{R} \to \mathbf{R}$

Florentin Smarandache, prof. ,Vâlcea

Rezolvare corectă:

$$fog(x) = f(g(x)) = \begin{cases} e^{g(x)}, & \text{dacă } g(x) \le 3 \\ e^{-g(x)}, & \text{dacă } g(x) > 3 \end{cases}$$

$fog: \mathbf{R} \to \mathbf{R}$

$$g(x) \le 3 \Rightarrow \begin{cases} x^2 \le 3 \Rightarrow x \in [-\sqrt{3}, 0] \\ sau \\ -2x+7 \le 3 \Rightarrow x \in [2, +\infty) \end{cases}$$

$$g(x) > 3 \Rightarrow \begin{cases} x^2 > 3 \Rightarrow x \in (-\infty, -\sqrt{3}) \\ sau \\ -2x+7 > 3 \Rightarrow x \in (0, 2) \end{cases}$$

$$\text{Deci } (fog)(x) = \begin{cases} e^{-x^2}, & x \in (-\infty, -\sqrt{3}) \\ e^{x^2}, & x \in [-\sqrt{3}, 0) \\ e^{2x-7}, & x \in (0, 2) \\ e^{2x-7}, & x \in [2, +\infty) \end{cases}$$

publicată, Gazeta matematică, nr.7/1981, Anul L XXXVI. pp. 282-283.

UNDE ESTE GREȘEALA? (sistem de inecuații)

Să se rezolve sistemul de inecuații:

$$\begin{cases} x \geq 0 & (1) \\ y \geq 0 & (2) \\ x - 2y + 3z \geq 0 & (3) \\ -3x - y + 4z \geq 4 & (4) \end{cases}$$

"Soluție". Înmulțim a treia inegalitate cu 3 și o adunăm la a patra. Sensul se păstrează. Rezultă:

$-7y + 13z \geq 4$, sau $z \geq \frac{1}{13}(7y + 4)$

Deci $x \geq 0$ și $y \geq 0$ (din inecuațiile (1) și (2)) și $z \geq \frac{1}{13}(7y + 4)$ (*). Dar $x = 13 \geq 0$, $y = 0 \geq 0$ și $z = 2 \geq \frac{4}{13} = \frac{1}{13}(7 \cdot 0 + 4)$ verifică (*), în schimb nu verifică sistemul de inecuații, deoarece înlocuind în a patra inecuație avem:

$-3 \cdot 13 - 0 + 4 \cdot 2 \geq 4$

ceea ce nu este adevărat.

Unde este contradicția?

Rezolvare.

Soluția anterioară este incompletă. Nu s-au intersectat toate cele patru inecuații. Dându-i o interpretare geometrică în $\mathbf{R}^3$, și scriind inecuațiile ca ecuații, avem de-a face cu patru planuri, fiecare împarte spatiul în semispații. Deci soluția sistemului o vor constitui punctele aflate la intersecția celor patru semiplane, (fiecare inecuație desemnează un semispațiu). Inecuația obținută prin adunarea inecuației a treia cu a patra nu reprezintă altceva decât un alt semispațiu care include soluția sistemului, și nu simplifică sistemul (în sensul că nu putem elimina nici una dintre inecuațiile sistemului).

Astfel $x = 0$, $y = 3$, $z = 5/13$ verifică (*) daŕ nu verifică, de data aceasta, inecuația a treia (deși pe a patra o verifică).

L'ILLOGIQUE MATHEMATIQUE!

Trouvez une "logique aux énoncés suivants:

(1) 4-5 ≈ 5!

(2) 8 divisé par deux est égal à zero!

(3) 10 moins 1 égale 0.

(4) $\int f(x)\ dx = f(x)$!

(5) 8+8=8!

Solutions:

Ces fantaisies mathématiques sont des divertissements, des problèmes amusants: elles font abstration de la logique courante, mais elles ont quand même **leur** "logique", une logique fantaisiste: ainsi

(1) s'explique si l'on ne considere pas "4-5" comme l'écriture de "4 moins 5" mais comme celle de "de 4 à 5"; d'ou une lecture de l'énoncé "4-5 ≈ 5": entre 4 et 5, mais plus près de 5".

(2) 8 peut être divisé par deux . . . de la façon suivante: ..., c'est-a-dire qu'il sera coupé en deux parties égales, qui sont égales à "O" au-dessus et au-dessous de la barre!

(3) "10 moins 1" peut s'entendre comme: les deux caractères typographiques 1,0 moins le 1, ce qui justific qu'il reste le caractere 0.

(4) Le signe sera considéré comme la fonction inverse de l'intégrale.

(5) L'operation " $\infty + \infty = \infty$" est vraie: on va l'écrire

verticalement: ∞

$+$

∞

$=$

∞

ce qui, transposé horizontalement (par une rotation mecanique des signes graphques) donnera bien l'énoncé: "8+8=8".

OPTICAL ILLUSION
(Mathematical Psychology)

What digit is it, 8 or 3?

[Answer: Both of them!]

1. EPMEK =Reverse of Kempe.

2. DEDE/KIND = DedeKind's cut.

3. B
R
O = Angle of Brocard.
C
A
R
D

4. BRIANCHON = Point of Brianchon

5. $\begin{vmatrix} \mathrm{SYL} \\ \mathrm{VES} \\ \mathrm{TER} \end{vmatrix}$ = Determinant of Sylvestor.

6. E A O T E E
  r t s h n s = Sieve of Eratosthenes.

7. A
R C
T S
D E S = Foliate curve of Descartes.

8. $\begin{pmatrix} \mathrm{MRX} \\ \mathrm{RAI} \\ \mathrm{XIT} \end{pmatrix}$ = Symmetrical matrix.

9. $\overline{\mathrm{SHEFFER}}$ = Bar of Sheffer.

10. □ □ □ □ = Method of the littlest squares.

11. $\begin{pmatrix} \mathrm{J}10000 \\ 0\emptyset 1000 \\ 00\mathrm{R}100 \\ 000\mathrm{D}10 \\ 0000\mathrm{A}1 \\ 00000\mathrm{N} \end{pmatrix}$ = Matrix of Jordan.

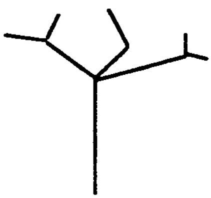
12. NOITCNUF = Inverse function.

13. SERUGIF = Inverse figures.

14.
R V R V
M K M K = Markov Chains.
A O A O

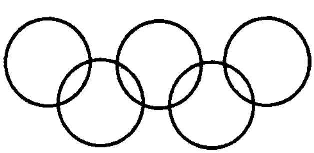
15. $\frac{\text{USA}}{\text{WEST EUROPE}}$ = Harmonious report.

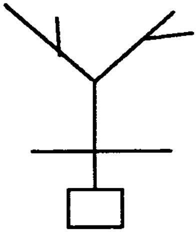
16. $\frac{\text{USA}}{\text{USSR}}$ = Anharmonious report.

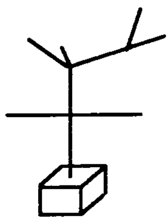
17.  = Tree.

18.  = Convergent filter.

19.
A
P S
O U = Circle of Apolonius.
L I
O N

20.  = Fascicle of circles.

21.  = Square root.

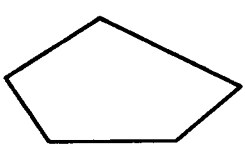
22.  = Cubic root.

23. $X^{\infty} + Y^{\infty} = Z^{\infty}$ = Fermat's last theorem!

24. I–W–A–S–A–W–A = Iwasawa's decomposition

25. R E

O M = Latin square!

26.  = The pentagon!

27. ∅ = Reductio ad absurdum.

28. O = Ring.

29. F N
U O
N I
C T

= Convex function.

30. P N S
I T
O

= Noncollinear points.

31. G
R P
O U

= Group of rotations.

32. ELEMENTS

= Nondisjoint elements.

33. M
X A
I T
R

= Circulant matrix.

34. O L
P I
N
O G

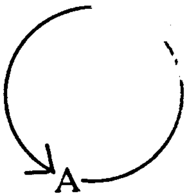
= 7-gon.

35. SPA
CE

= Compact space.

36. A
L
G
E
B
R
A

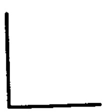
= Higher algebra.

37. 

= Vicious circle.

38. A
R
I
T
H
M
E
T
I
C

= The higher arithmetic.

39. 

= Square angle.

40. SYMBOL OF (LEOPOLD) KRONECKER = L.K.

41. KOLMOGOROV'S SPACE = USSR.

42. LANGUAGE OF CHOMSKY = American.

43. GRAMMAR OF KLEENE = English.

44. CATASTROPHIC POINT = Atom bomb.

45. MACHINE OF TURING = Motor car.

46. NUMBER OF GOLD = 79 (chemically).

47. FLY OF LA HIRE = Insect.

48. MOMENT OF INERTIA ≐ Apathy.

49. AXIOM OF SEPARATION = Divorce.

50. CLOSED SET = Prisoners.

51. RUSSIAN MULTIPLICATION = Conquest.

52. SLIPS OF MÖBIUS = Bathing trunks.

53. SINGULAR CARDINAL = Mazarin (1602-1661, France).

54. CLAN OF LEBESGUE = His family.

55. SPHERE OF RIEMANN = Head.

56. MATHEMATICAL HOPE = Fields prize.

57. CRITICAL WAY = Slope.

58. BOTTLE OF KLEIN = Beer bottle.

59. CONSTANT OF EULER = Mathematics.

60. CONTRACTANT FUNCTION = Frost.

61. BILINEAR COMBINATION = Concubinage.

62. HARDY SPACE = England.

63. INTRODUCTION TO ALGEBRA! = AL.

64. INTRODUCTORY ECONOMETRICS = ECO.

65. BOREL BODY = Corpse.

66. CHOICE FUNCTION = Marriage.

67. GEOMETRICAL PLACES = ATHENA, ERLANGEN etc.

GAMMA, anul IX, nr.1, noiembrie 1986

LOGICA MATEMATICĂ

Câte propoziții sunt adevărate și care anume dintre următoarele;

1. Există o propoziție falsă printre cele n propoziții.

2. Există două propoziții false printre cele n propoziții.

- -

... Există i propoziții false printre cele n propoziții.

- -

n. Există n propoziții false printre cele n propoziții.

(O generalizare a unei probleme propuse de prof. FRANCICO BELLOT, revista NUMEROS, nr. 9/1984, p. 69, Insulele Canare, Spania)

Comentarii

Notăm cu P_i propoziția i , $1 \leq i \leq n$. Dacă n este par atunci

propozițiile 1,2,...,($n/2$) sunt adevărate iar celelalte false. (Se începe raționamentul de la sfârșit; P_n nu poate să fie adevărată, deci P_1 este adevărată; apoi P_{n-1} nu poate fi adevărată, deci P_2 este adevărată, etc.

Remarcă. Dacă n este impar se obține un **paradox**, deoarece urmând aceeași metodă de rezolvare găsim P_n falsă, implică P_1 adevărată; P_{n-1} falsă implică P_2 adevărată, ... $P_{\frac{n+1}{2}}$ falsă implică $P_{n+1-\frac{n+1}{2}}$ adevărată, adică $P_{\frac{n+1}{2}}$ falsă implică $P_{\frac{n+1}{2}}$ adevărată, absurd.

Dacă $n=1$, se obține o variantă a Paradoxului mincinosului ("Eu mint" este adevărat sau fals?)

- -

1. Există o propoziție falsă în acest dreptunghi.

- -

Care este desigur un paradox.

PARADOXE DES AXES RADICALES

Propriété: Les axes radicals de n cercles d'un même plan, pris deux à deux, dont les centres ne sont pas alignés, sont concourants.

"Demonstration" par recurrence sur $n \geq 3$.

Pour le cas $n = 3$ on sait que 3 axes radicals sont concourants en un point qui s'appelle le centre radical. On suppose la propriété vraie pour les valeurs inférieures ou égales à un certain n.

Aux n cercles on ajoute le (n+1) è cercle.

On a (1): les axes radicaux dès n premiers cercles sont concourante en M.

Prenons 4 cercles quelconques, parmi lesquels figure le (n+1) è.

Ceux-ci ont les axes radicals concourants, conformémént à l'hypothèse de récurrence, et au point M (puisque le 3 premiers cercles, qui font partie des n cercles de l'hypothèse de récurrence, ont leurs axes radicals concourrant en M).

Donc les axes radicals des (n+1) cercles sont concourants, ce qui montre que la propriété est vraie pour tout $n \geq 3$ de /N.

ET POURTANT, on peut constrire le.

Contre-exemple suivant:

On considere le parallélogramme ABCD qui n'a aucun angle droit.

Puis on construit 4 cercles de centres respectifs A,B,C et D, et de même rayon. Alors les axes radicals des cercles e (A) et e (B), respectivement e (C) et e (D), sont deux droites, mediatrices respectivement des segments AB et CD.

Comme (AB) et (CD) sont paralléles, et que le parallélogramme n'a aucun angle droit, il en resulte que les deux axes radicals sont paralléles ... c'est-à-dire qu'ils ne se coupent jamais.

Expliquer cette (apparente!) contradiction avec la propriété anterieure?

Reponse: La "propriete" est vraie seulement pour n=3. Or dans la démonstration proposée on utilise la premisse (fausse) selon laquelle pour m+4 la propriété serait vraie. Pour achever la preuve par récurrence il faudrait pouvoir montrer que $P(3) \Rightarrow P(4)$, ce qui n'est pas possible puisque P(3) est vraie mais que le contre-exemple prouve que P(4) est fausse.

SMARANDACHE CLASS OF PARADOXES

Let A be an attribute and non-A its negation.

P1. ALL IS "A," THE "NON-A" TOO.
Examples:
E_{11}: All is posssible, the impossible too.
E_{12}: All is present, the absentee too.
E_{13}: All is finite, the infinite too.

P2. ALL IS "NON-A, "THE "A" TOO.
Examples:
E_{21}: All is impossible, the possible too.
E_{22}: All is absent, the present too.
E_{23}: All is infinite, the finite too.

P3. NOTHING IS "A" NOT EVEN THE "A."
Examples
E_{31}: Nothing is perfect, not even the perfect.
E_{32}: Nothing is absolute, not even the absolute,
E_{33}: Nothing is finite, not even the finite.

Remark: P1 $\Leftrightarrow$ P2 $\Leftrightarrow$ P3.

More Generally: ALL (verb) "A." the "NON-A" too.

Of course, from these there are unsuccessful paradoxes, but the proposed method obtains beautiful ones.

Look at a pun, which reminds you of Einstein:

All is relative, the (theory of) relativity too! So:

The shortest way between two points is the meandering way!

The unexplainable is, however, explained by this word: "unexplainable!"

Tipar: grupul drago print

TIPOGRAFIA FED Calea Rahovei 147,
sector 5 - București; Tel.: 335.93.18; Fax: 337.33.77

ISBN 973-9205-02-X

Preț: 10 000 lei